Oxford Internet Institute Forum Discussion Paper No. 17, 1 March 2010

Child Protection and Freedom of Expression Online

Alison Powell, Michael Hills and Victoria Nash

Oxford Internet Institute
University of Oxford
March 2010

Advocates of online child protection and freedom of expression share a deep-seated belief in the importance of protecting basic human rights. Yet these beliefs are often clouded by perceived (and real) opposition in the actual practice of law, policy, and regulation. This has restricted the policy options available for dealing with threats to both child safety and free speech online, and has often resulted in these interests being portrayed as diametrically opposed. Advocates on both sides of this debate met in Oxford in October 2009 to explore their different perspectives on these fundamental rights and to identify possible areas of agreement. By defining a new framework to discuss online child protection that rejects the current moral panics that have dominated the debate, and focuses instead on accurately defining risks in line with the evolving capacity of the child, participants were able to find some common ground. The most fruitful avenues came from calls for precision and transparency in policy responses that touch on these issues. Participants discussed how, by working together, both sides could advance their agendas and defend the rights of children while preventing child protection from being used as a strategic pretext for broader goals of censorship and repression.

Introduction

> States Parties undertake to ensure the child such protection and care as is necessary for his or her well-being, taking into account the rights and duties of his or her parents, legal guardians, or other individuals legally responsible for him or her, and, to this end, shall take all appropriate legislative and administrative measures.
>
> Article 2 UN Convention on the Rights of the Child

> The child shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice.
>
> Article 13 UN Convention on the Rights of the Child.

Many think of the Internet as being an adult medium into which children and legal minors occasionally intrude. However, this is not necessarily the case. Hundreds of millions of children and young people around the world are regular and active users of the Internet. Their rights, as defined by national and international law, should be considered in any discussion of law, policy, or regulation on the Internet.

Under the United Nations Convention on the Rights of the Child and in several other international instruments, as well as within the national laws of almost every country that is a member of the UN, it is accepted that children are continually developing and learning as they grow up. It is recognised and accepted that this developmental process has consequences for children’s capacity to identify, assess, and manage potential risks. The Convention and national laws therefore establish that children have a legal right to be protected from all forms of exploitation. This includes exploitation in cyberspace, just as it covers exploitation in the real world.

At the same time, both children and adults enjoy other well-established rights such as free speech or free expression rights, which are also protected by instruments of national and international law, but which may appear to conflict with protective measures limiting access to certain sorts of online material or activities.

Given these conflicts, law, policy, and regulation that seeks to protect both sets of rights on the Internet becomes a question of balance. How can children's rights to protection be realised on an anonymous global network where anyone can communicate with anyone else? Do these rights to protection inevitably lead to the limitation of other well-established rights, such as free speech or free expression? Is there a system that can reconcile the two sets of rights or at least deliver an acceptable balance? Will an interest in protecting rights lead to excessive state interference, or is the state ultimately responsible for the well-being of the most vulnerable? Not everyone agrees on the answers to these questions.

Advocates of online child protection and freedom of expression both share a deep-seated belief in the importance of protecting basic human rights, grounded in fundamental values of human autonomy and dignity. Yet a shared belief in the importance of protection of core human freedoms is often clouded by perceived (and real) opposition in the actual practice of law, policy, and regulation. This has consequently restricted the policy options available for dealing with threats to both child safety and free speech online, and has often resulted in the interests of child protection and freedom of expression advocates being portrayed as diametrically opposed.

Given the significance of the values that both sets of advocates protect, and the increasing importance of defending these values in fast-moving international discussions about Internet governance, the Oxford Internet Institute (OII), set about to explore the range of underlying principles in both movements in order to map the territory and determine limitations of any potential common ground.

In October 2009, panellists from organisations on both sides of this debate met in Oxford to present position papers that mapped the terrain of disagreement, and to explore the potential for reconciling these fundamental rights, especially within policy and regulation. The following report is an attempt to synthesise the debate held during that meeting and to make the case for further conversation and collaboration. The goal of this forum was to start a conversation and restructure the framing of a historically divisive debate, and as such, it is important to note that what follows makes no specific policy recommendations.

Framing the Debate—Past Perspectives

> At any moment, those same kids exploring jungle fauna or listening to ... Baby One More Time are just a few keystrokes away from Pandora's hard drive--from the appalling filth, unspeakable hatred and frightening prescriptions for homicidal mayhem.[1]
>
> Time Magazine, 1999

Child protection advocates and freedom of expression advocates have traditionally been framed as being diametrically opposed and have rarely, if ever, been brought together to discuss the issues addressed at this forum. The truth, however, is that organizations and individuals on both sides of the debate express nuanced points of view that protect both sets of values.

Whilst there may be genuine and significant sources of disagreement, both child protection and freedom of expression advocates are often frustrated and under-served by the framework typically used in popular discussion and media reports, as well as by some elected officials, when addressing the issue of young people online. This framework is based largely on fear and focused on violent sexual harm resulting from use of the Internet.

Youth use the Internet as a communication medium as well as a way of receiving information and media. In this context, the fixation on explicit chat and solicitation online is not necessarily in touch with actual practices—thus taking on the characteristics of a moral panic. A popular North American news journal television show, Dateline NBC, declared incidents of adults engaging in sexual chat and solicitation with minors a ‘national epidemic’ and launched a regularly running, highly rated special investigative series called ‘To Catch a Predator’, in which the show's producers set up sting operations to catch online sexual deviants in the act (Rickert and Ryan, 2007). The US Department of Justice, in a news conference complete with uniformed federal agents, warned that ‘seemingly friendly Web sites like MySpace or Facebook often are used by sexual predators as victim directories’ (Wolak et al., 2008).

This sense of moral panic is not confined to the United States. Hasebrink, Livingstone, and Haddon find that over one third of newspaper articles in the UK, Belgium, Spain and Greece

[1] See: http://www.time.com/time/magazine/article/0,9171,990919,00.html

discussing online threats and opportunities are dominated by concerns over sexual content and solicitation (Hasebrink, Livingstone, and Haddon, 2008).

The biggest problem with the moral panic framework is that it can over-represent the likelihood of harm that children face online and presents an image of the Internet that does not reflect the experience of most children (Finklehor[2]). In doing so, it obscures and undermines the work of both freedom of expression and child protection advocates. It leads to false conclusions about the motives of freedom of expression advocates, and misrepresents the considered actions by many child protection groups to identify and combat actual risks that children face as they access the internet on a daily basis.

In working to protect freedom of expression online, freedom of expression advocates consistently find themselves accused of ignoring the plight of children. Instead of discussing the value and benefits of freedom of expression and thought in a free democratic society, or protecting those rights from unnecessary government restriction, they often find themselves fending off critics who use the moral panic framework and examples of the worst kinds of inflammatory, violent, sexist, and racist material to argue that freedom of expression advocates lack a moral base or code. In addition, these accusations are often amplified with an emotional appeal to 'think of the children', thus presenting a tacit insinuation that those who value freedom of expression are indifferent to the needs of the more vulnerable in society.

This pressure can be clearly seen in recent comments by Brad Templeton, Chairman of the Board for the Electronic Frontier Foundation (EFF) when asked about the erosion of digital rights:

> It's kind of a scary thing to talk about because they deliberately use this as a wedge issue, but there are these boogie men of the modern era, which are the child molesters, kiddie porn, that sort of people, and nobody thinks they're not terrible people, and nobody thinks it's not something that should be stopped, however, what happens is one side seems to always sort of portray that unless we do what they want to do in order to stop terrible things, that you must be therefore in favor of the terrible things, which is not how it works. That means we see proposals to do things like monitor the entire Internet to make sure that nobody is sending the wrong images over it, and if you say you don't like that, they think, why, do you want to help the kiddie pornographers? And obviously, no, we don't want to help the kiddie pornographers, but you also don't like the idea of putting that level of surveillance on the network, because it has so many terrible potential misuses.[3]

In other words, implying that the work of free speech advocates supports reprehensible actions instead of protecting essential liberties runs the risk of closing off dialog between freedom of expression advocates and child protection advocates—the majority of whom do not advocate measures for child protection as a justification for limits on freedom of expression.

The current framework of debate also has negative consequences for many child protection advocates. In fighting to protect the rights of children online, child protection advocates are sometimes unfairly aligned with those responsible for the moral panic, and are unjustly accused as dismissive of civil liberties. Considered and reasoned positions on filtering, age verification, law enforcement, and education based on empirically validated risks are often distilled into accusations that the true goal of child protection advocacy is a censored and monitored Internet

---

[2] See: http://www.unh.edu/ccrc/internet-crimes/

[3] See: http://memebox.com/futureblogger/show/6-eff-chairman-templeton-expect-more-repression-of-rights-in-2008-via-audio-transcript-

where every page has been vetted and pre-approved for society's youngest or most vulnerable members.

These accusations are illustrated by recent debates where opponents have accused child protection advocates of ‘getting into thought control’, ‘wanting a nanny state’, and wanting minors to have ‘veto power over the Internet’.

The moral panic framework has proven unhelpful for both child protection and freedom of expression advocates and has led to the misrepresentation and co-opting of both agendas.

In planning our forum, we found that freedom of expression advocates insist that they are deeply concerned about protecting children online, arguing that a safer Internet would mean less pressure to limit freedom of expression rights in addition to being a useful goal in itself. We also found that child protection advocates are as passionate about children’s positive rights to freedom or expression as they are about protecting them from harm. Perhaps most importantly, both groups identified that the division between them is often exacerbated by others who would use child protection as a ‘strategic pretext’ for broader goals of repression and censorship—thus ‘co-opting’ the debate.

At the level of broad rights, child protection and freedom of expression advocates do share some similar values and concerns. Important differences remain about how these values should be balanced, and who should take responsibility for them, but these can most fruitfully be addressed if it is acknowledged that there is also common ground. To clarify and build on this common ground, however, a new framework for the discussion of child protection online needs to be found.

New Framing—Risks and Benefits

> By narrowing the ground we will force totalitarian regimes to justify their repression for what it is—and that is nothing to do with child protection.
>
> John Carr

In trying to map areas of common ground, both the child protection advocates and the freedom of expression advocates we consulted supported a move away from the framework of moral panic to one based on a more accurate understanding of the risks and benefits that the Internet poses for children, a more precise language in the description of these risks and opportunities, and a closer look into the unintended consequences that well-meaning law, policy, and regulation can have on civil liberties.

Whilst always being mindful of the tragic reality behind the headlines that refer to solicitation cases involving paedophiles, or to children driven to suicide, it was accepted that an emphasis on the extreme, violent, or deceptive stranger archetypes can mask and distract from much more prevalent risks.

Fortunately, there is reason for optimism. Recent work by scholars throughout North America and Europe has advocated a better framing of this debate and provided solid empirical evidence to support its call. Examples of excellence in this field cited by those in our forum include Sonia

Livingstone's work with the EU Kids Go Online Project,[4] the Berkman Center's 'Enhancing Child Safety and Online Technologies',[5] and David Finkelhor's work as the director of the Crimes against Children Research Center[6] at the University of New Hampshire.

These three research initiatives all reach a similar conclusion: that the risks children face online are not significantly different from those they face offline. Each concludes that the stereotype of deceptive paedophiles committing forcible sexual assault is comparatively rare, but that there are still risks of varying degrees for children online. Significantly, all three claim that the risks are not the same for all children, and that psychological makeup and family dynamics are better predictors of risk than access to technology or time spent online. Other common conclusions suggest that risks online are most prevalent for children with a history of sexual abuse, drug and alcohol abuse, sexual orientation concerns, or risk-taking behaviour, and that online threats change as children age and develop.

There was common agreement by the forum participants that if a new framework for discussion was to be found—one that would enable the mapping of common ground—it was most useful to agree on two points: first, that all risks are not equal, and second, that experience of risk is individual.

1. All Risks are Not Equal (Different risks may require different actions).

One useful distinction between risks was provided by Sonia Livingstone, who identified four types of risks: commercial risks (advertising, spam, phishing, or the collection of personal data), aggressive or violent risks (bullying or exposure to violent content), sexual or sexually harmful risks (child sex abuse images, predation and solicitation, grooming, or the exposure to pornography), and values-based risk (such as misleading advice, the encouragement of self harm, or racist and hate speech). Livingstone further distinguished between types of risk by suggesting that children could encounter each type of risk in one of three ways: as recipients, in the case of content risks, where children are relatively passive in the encounter; as participants, in the case of contact risks, where children are active in the encounter, though not necessarily the initiators; and as initiators, in the case of conduct risks, where children are the perpetrators of the risk.

2. Risk is Individual, Personal and Can Change over Time (Risks can be reduced but not eliminated, and risks need to be measured against corresponding opportunities in determining what action, if any, needs to be taken).

Both points stress the importance of precision in policy making. In the past, a refrain of 'think of the children' has been used by the media and by some elected officials to call for broad-stroke responses that have unintended consequences for both adults and children. These responses rarely help anyone in the long run, and can lead to broad freedom of expression repressions that are often, particularly in the US, defeated in practice or through the courts. This does nothing to mitigate the original risks to children.

Using risk classifications, it becomes possible to bring precision to the language used in discussing the experience of children online. This precision, in turn, allows discussion on law, policy, and regulation that targets specific, identifiable risks. By targeting specific points of risk, child protection advocates can offer reasonable workable solutions that are much more likely to find support among freedom of expression advocates. By working together, both groups can help make children safer while avoiding broad restrictive policies that run a risk of infringing on

[4] http://www.lse.ac.uk/collections/EUKidsOnline/Default.htm

[5] http://cyber.law.harvard.edu/pubrelease/isttf/

[6] http://www.unh.edu/ccrc/researchers/finkelhor-david.html

the freedom of expression rights of both children and the wider public. The better we can define the risk, the easier it becomes to strike a balance between the risks and opportunities provided by the Internet.

The Benefits of Internet Use

As well as seeking clarification of the risks of Internet use, forum participants were quick to point to its benefits. Advocates of child protection may often be depicted as aiming to restrict access for minors, but all present at the forum agreed that the Internet presented a wealth of opportunities for young people and children. Its value as a social as well as educational tool was emphasised by all, and the importance of finding measures which did not restrict access was a point of consensus. Even those from child protection groups who were more comfortable with the prospect of filtering content were keen that the filtering process should be minimally intrusive, and as finely tuned as possible to avoid scenarios where minors could not access or discuss material about—for example—breast cancer or sexual health. With this in mind, any suggested framework that would further debate in this area should emphasise the broad range of benefits of Internet use, of which freedom of expression would be a vital but not sufficient component.

With this alternative framework in mind, the participants at the forum discussed specific issues that have come to dominate any discussion of the balance between child protection and freedom of expression online. In this more specific discussion, areas of clear dissent emerged, which connected with the values of different advocates as well as their positions on the roles of government, family, and other actors within the debate.

Specific Issues

Blocking and Filtering

One frequently proposed solution for protecting children online is the blocking or filtering of online content. Filters or ‘parental controls’ can be installed on an individual computer or configured at the ISP level. At a higher level, ISPs can block content originating from specific IP addresses that are found to be distributing content such as child abuse images. In some jurisdictions lists of these sites are maintained by third-party organizations, and ISPs voluntarily agree to comply with them.

There were significant divergences of opinion on the both the efficacy of filtering and the responsibility for filtering. We found that agreement or differences of opinion on this topic came down to questions of what was being blocked or filtered, who was doing the blocking or filtering, and at what level the blocking or filtering was being carried out.

For this reason, we found it useful to structure our discussions around types of conduct (illegal for all, illegal for minors but not adults, legal but perhaps distasteful or controversial), sources of filtering or blocking parameters (government, NGOs, ISPs, private companies, individuals), and points of control (backbone, ISP, individual networks, individual homes).

The strongest consensus was found in the discussion of blocking access to content that was patently illegal for all, the most clear-cut example of this being child sexual abuse images. Child sexual abuse images are illegal in most jurisdictions, and there was almost unanimous agreement that the voluntary blocking of these images at the ISP level was acceptable and

appropriate. Dissent on this point concerned the ability of or justification for ISPs to determine whether content was illegal, and the transparency of block lists if these were used. It was also noted that there are other types of content, such as hate speech, which are illegal in some jurisdictions, but which are open to much greater controversy.

Although a contentious issue, most participants agreed in principle that in a competitive market, there was nothing inherently wrong with an ISP providing mandatory filtering of any content, since subscribers would be willingly choosing this service over the others available. However, this does not necessarily mitigate the problems with delegating responsibility to ISPs for arbitrating illegal content.

Higher-level filtering and government responsibility for filtering was even more contentious. While some child protection advocates insisted that government-mandated filtering at the backbone level was justifiable if it would more effectively reduce access to child abuse images, most freedom of expression advocates believed that any government-mandated filtering or blocking was too great an infringement on civil liberties. In particular, there was disagreement regarding the fundamental role of government, with some seeing it as the trusted first-line defence of individual rights, and others adopting a more libertarian position in which government intervention should be minimised and constantly scrutinised.

The extent to which individual parents or families could restrict access to content for their children was surprisingly controversial. There was general agreement that filters could be useful tools for parents, but there was a clear division of opinion on who should set the defaults of filters. Groups whose primary focus was child protection argued that filtering software should come pre-installed and pre-configured to the highest setting on all home computers, while those whose primary focus was freedom of expression believed that using a filter should be a personal choice, and that overly restrictive default settings could be damaging to free expression. There was also dissent about which entities should be responsible for mandating defaults and the consequences of making the state, parents, or ISPs finally responsible for filtering decisions.

While everyone agreed that parents or individuals should have the right to change settings or completely remove filtering, there was a clear ideological split on the influence of the starting point for filters, and whether default settings would influence subsequent behaviour. In addition, different jurisdictions have different perspectives on what kind of content should be filtered: for example, some child protection advocates argue that non-photographic images of children, or ‘pseudo’ images, should be filtered, whereas in other jurisdictions such images are subject to free expression protection. In a related example, the United States treats ‘harmful to minors’ speech as fully protected for adults.

Throughout the discussion on blocking and filtering, it became clear that both child protection and freedom of expression advocates considered transparency to be a fundamental prerequisite in any implementation of filtering. There was unanimous agreement that, regardless of individual opinions on what should be filtered where and by whom, transparency is important. There should be no room for doubt or suspicion about how a site gets on a filtered or blocked list, there should be clear review procedures for being removed from the list, and lists should be consistently reviewed and updated. In addition, anyone attempting to visit a site that has been filtered or blocked should be informed that the site has been filtered or blocked, why and by whom the site has been filtered or blocked, and what the process is (if any) for removing the site from the filtered or blocked list. There was also agreement that for filtering or blocking to be transparent it should be specific and targeted. In particular, there was strong consensus that child sexual abuse images should be blocked, but much dissent about the responsibility for locating these images and determining their provenance.

In many ways, these concerns about filtering are complicated by great variation in national perspectives on blocking and filtering, and the limited comparative data on actual use of filters in different jurisdictions—not to mention the ease of circumventing filters. Still, the OII's Oxford Internet Surveys (OxIS)[7] indicate that 97% of UK residents believe that it is the parents' responsibility for restricting Internet content., but only 36% actually used filters In the United States however, the Children's Internet Protection Act requires libraries to install filtering software in order to receive government subsidies for equipment and connectivity. Freedom of expression advocates raise concerns that such filters could limit access to information, since some filters can remove legitimate information covering topics such as health or sexuality. Concerns about the responsibility for determining which content would be filtered highlighted the importance of transparency, especially in libraries. Some free speech advocates argued that without this transparency the unintended consequences of filtering could be amplified: library patrons for example might come to believe that filtered information was simply unavailable.

On the other hand, child protection advocates argued that filtering was necessary to limit the propagation and circulation of child abuse images, especially since each abuse image constituted a revictimization of a child. Child protection advocates also acknowledged that there are many child abuse images that have been circulating for years online.

Government Legislation and Law Enforcement

The role of the state and of law enforcement were contentious. There was general consensus on the importance of supporting law enforcement in investigating and prosecuting illegal activity, but much disagreement about the extent to which this should be connected with broader state activities. While acknowledging the fact that child protection online and child protection offline are not mutually exclusive endeavours, most participants felt that it would of course be better and preferable if governments could be more effective at stopping illegal activity in the first place or apprehending the perpetrators, as opposed to blocking and filtering the online content. Blocking and filtering illegal content was a secondary value and shouldn't take priority over prevention. The child protection advocates saw it as a necessary practical response to an immediate practical problem.

Several participants argued that by staying out of the filtering and blocking arena entirely, law enforcement agencies would have more time and resources to dedicate to finding and stopping those producing and disseminating child sexual abuse images. Others, however, were quick to point out that the repeated assessment of the legality of the same images is a drain on resources, and that where the technology existed to electronically match known child sexual abuse images and then block access to those images, such technology should be used to prevent the re-victimisation of the abused and allow law enforcement to focus on new cases.

Participants stressed that international standards vary considerably in terms of the presence or quality of legislation. Many countries now have clear and effective child protection legislation, but in other areas very basic steps still need to be taken, with many countries having no laws whatsoever against child sexual abuse imagery at all, not to mention provisions for online safety. For example according to John Carr, in several countries it is still technically impossible to commit certain crimes against children online because the existence of an intangible place, such as cyberspace, is not recognized as a locus within which such crimes can be committed.[8]

---

[7] See: http://www.oii.ox.ac.uk/microsites/oxis/

[8] International Centre for Missing & Exploited Children (2008). Child Pornography: Model Legislation & Global Review. Fifth Edition. Available at: http://www.icmec.org/missingkids/servlet/PageServlet?LanguageCountry=en_X1&PageId=3085

The existing legislation on child sexual abuse and predation has evolved a precise language and appropriate and proportionate responses, which was one element that our participants agreed was a key to ensuring its effectiveness. There was shared concern, however, about trends towards new legislation and law enforcement that is less precise since this could lead to responses that are confused and disproportionate. Some of the issues and practices associated with these emerging legislative and law enforcement movements are described by the buzzwords 'sexting' and 'cyber-bullying'.

Cyberbullying

Our participants agreed that cyber-bullying could not be separated from bullying in general. While acknowledging that the Internet allows bullies to extend their reach and create a permanent record of their bullying, it was agreed that there is no legislative or law enforcement distinction to be made between bullying online and bullying offline. The social conditions that give rise to bullying and the risk factors that are predictive of harm are the same in the two environments; attempts by legislators and law enforcement to separate the issues are misguided. Therefore efforts to curb cyberbullying should be pursued through a strategy of understanding and preventing bullying in general.

Sexting

Participants also agreed on the importance of stepping back from moral panics about sexting, the sending of sexually explicit text or instant messages. Fear of sexting has elided the difference between predatory actions involving criminal interactions between adults and children, and innocent—though perhaps inappropriate—interactions between children and their peers. At its worst, the term 'sexting' undermines both those advocating for child protection and those advocating for free speech, as it opens the door to criminalizing peer-to-peer communication by equating it with established, clear-cut illegal activity. Remarked a participant: 'When a forty-year-old man sends a picture of his genitals to a fourteen-year-old girl, it's not sexting, it's a crime'.

The confusion about the legal status of sexting, particularly between peers, is exacerbated by overzealous law enforcement and vague legislation. Participants noted that while some law enforcement agencies, such as the British police, have taken a common-sense approach and decided not to criminalize consensual peer-to-peer contact, some classic disproportionate responses have been seen in other jurisdictions. As an example, a recent case in the United States resulted in six Pennsylvania high school students being charged with distributing or possessing child pornography in relation to the consensual texting of semi-nude photos of themselves to each other. A similar case in Ohio lead to a weekend incarceration for a 15 year old girl and the demand by a state legislator that she be forced to register as a sex offender.

Precision in Policy-making

The line separating inappropriate conduct from illegal conduct is easily blurred, and different participants disagreed on the shades of grey between the two, but all agreed that precision on the issue is needed and that law enforcement action should use this precision to gauge the proportion of their response. It was also agreed that children's interests are best served when legislation remains targeted to reducing the largest risks. Legislative efforts are undermined when the claim to protect children is used as a smokescreen for keeping adult content from adults or by those who wish to limit children's exposure to diverse ideas that carry little or no risk.

Many at the forum were not optimistic that this precision or commitment to minimal invasiveness could be found, based on their experiences of the policy-making process. Several forum

members pointed out that very often, child protection legislation is hijacked by those advocating stricter measures on computer fraud, intellectual property, or national security.

Targeted policy measures directed at reducing a specific risk within specific group can also fall victim to 'mission creep' where legislators aim to expand the scope of an idea in the hopes of expanding its benefit. Well-reasoned and narrowly directed proposals can turn into overly broad legislation based on reasoning that more is better—this is expressed in the belief that if some safeguards are good, more must be better, or that if one group can be shown to benefit from a policy, all groups could benefit from an expansion of the same policy. For example, in the United States, the goal of protecting children from bullying—a very real risk—has been translated into legislation calling for the criminalization of all electronic communication meant to 'coerce, intimidate, harass or cause substantial emotional distress' to any person. By expanding the scope to this degree and criminalizing vague actions, the legislation opens itself to misinterpretation, misapplication, and unconstitutional rulings. All the while, the initial goal of reducing the risks of bullying barely advances.

Parental Involvement and Education

We had anticipated a clear consensus and uncontroversial discussion surrounding parental involvement in protecting children online and the importance of education for both parents and children, but the reality proved to be more complex.

No one disputed the importance of 'parental involvement' and 'education', but child protection advocates noted that these phrases shift the focus away from other means of protecting children. Since systemic factors such as poverty or risk of harm from parents already influence child safety online, there were some concerns that delegating responsibility to parents was tantamount to not addressing child safety at all. Other concerns identified that programmes that focus on education can increase the divide between the information-rich and information-poor, and that the greatest benefits of these programmes are often missed by the most at-risk children. Child protection advocates believe it must be acknowledged that parental involvement and education may not adequately combat the risks children face online.

The State's Responsibility

There was considerable debate on the levels of responsibility and limitation that should be placed on states as the children's caregiver of last resort, and it was noted that any intervention would have to be culturally sensitive and in keeping with specific regulatory regimes. Signatories of the United Nations Convention on the Rights of the Child extend certain rights to children, such as the right to free expression and the right to access information of their choice, in keeping with their level of maturity and experience. Conversely, in the United States, which is not a signatory to the Convention, the Fifth Amendment, which covers both freedom of expression and the right to family self-determination, has been interpreted by the courts as giving parents the right to direct and control the upbringing of their children.

Despite the debate, it was acknowledged that for the majority of children, parental involvement and education could play a large role in mitigating online risk. It was also noted that in carrying out this responsibility, some parents would turn to technological tools such as filtering programs to assist them. Since there are a wide variety of these tools, it was agreed that both child protection goals and freedom of expression goals were served by a belief that if filters are going to be used, they ought to be 'good' filters.

'Good' Filters

Debate emerged about how to define a 'good' filter: this included determining who should be responsible for the filtering, whether it could or should be mandated by a state or ISP, and how transparent it should be about what content was filtered and how this was determined. Some consensus emerged about the nature of 'good' filters: they should be easy to install, but also easy to disable by their owners; they should be transparent in terms of what they cover and why they are filtering particular content; and they should allow for changing conditions in line with the evolving capacities of their users. Filters should serve the expressed needs and desires of the user, and should not infringe on a user's privacy by tracking, logging and reporting usage to the software providers.

The group discussed whether the development of kitemark or trustmark system visually identifying filters that met certain conditions could be helpful for encouraging parental decision-making. While efforts for just such a system are underway in some countries, there was concern about the oversight of the development of such system. At a minimum, any system should employ neutral labelling of content, a published methodology for testing, and a strict renewal schedule for any kitemark awarded. Within this discussion, there was continued dissent about the level of responsibility that either governments or corporations should hold for determining filter default settings.

'Good' Education Programmes

Participants were clear that they were in favour of educational programmes for parents and children, as well as support for parents with a desire to mitigate risk, but pointed out that resources need to be reallocated to programmes that work. In order to do this, legislators need to understand the reality of the situation, target specific risks and the specific groups most likely to face those risks, and set aside time and money to assess the effectiveness of educational programs. There was much debate about how this process should work.

There was a general consensus among participants that there is currently no way of judging the efficacy of educational programs. It was agreed that educational programs tend to be large scale, untargeted, and not always based on the reality of the situation. It was also stated that there is rarely a budget or mandate to judge the effectiveness of such programs.

Research

As discussion progressed, it became clear that if governments want to make reducing risk online a priority, then they need to provide funding for research that provides empirical results about these risks. Such research supports the agenda of both child protection and freedom of expression advocates, as it identifies the causes of preventable harm and tracks the damage to civil rights that can result from unfounded assumptions or misused data. No country currently has a research agenda or strategy in this field. Thus, current research has effectively been ad hoc, with funding pieced together by committed researchers.

It was agreed by all that more research work needed to be undertaken on understanding children's online risks. The groundwork for this has been laid by recent contributions in reframing the debate made by Sonia Livingstone's work with the EU Kids Go Online Project, the Berkman Center's 'Enhancing Child Safety and Online Technologies', and David Finkelhor's work as the director of the Crimes Against Children Research Center at the University of New Hampshire.

There was less agreement, however, on what actions should be taken in the meantime. Child protection advocates insisted that while they inform their positions and programs with whatever research is available, there is often no time to wait for all the evidence to come in. If large

numbers of children are being harmed every day we all have a duty to use reasonable judgement about how best to combat it. Child protection advocates also queried the notion of 'precision' in research in this area. They pointed out that there are well-known difficulties in getting children to disclose stressful or traumatic experiences. For this reason they argue that risk to children may be underestimated or at least misunderstood.

Freedom of expression advocates argued that while it often appears that research seems to play little role in policy makers' decisions, it does play a major role in the judicial oversight of legislation. As courts will often look to ensure that the least-restrictive means of targeting a risk is used, it is important to properly quantify such risk and define precisely to which segments of the population the risk applies.

There was agreement, if little optimism, on the importance of developing new methodologies for assessing both risk and opportunities for children online. There was a general desire to create improved links between researchers and the legal, medical, and commercial sectors. Participants suggested that small changes to the way each collects information could go a long way in improving the available research. Law enforcement, for example, could record whether or not a computer or Internet connection was involved in cases they investigate. Voluntary commercial data panels such as ComScore could easily add metrics that measure risky online behaviours.

In assessing current research trends in child protection, we discovered improvement in some areas and continuing challenges in others. The good news is that traditional survey and interview methods have been strengthened by the work of Livingstone, Finkelhor, and others who have been sharing methodologies in an attempt to standardise a set of best practices that will both expand our current knowledge and make cross-study comparisons possible. The news, however, is not all good: for example, it was mentioned that new ways of tracking harm to children using media monitoring have become less accurate and in some cases useless, as the national media (and increasingly, even local media) have stopped reporting every instance of children coming to harm from interactions online.

Emerging Issues

Key emerging issues were the shared responsibilities of governments and parents in balancing freedom of expression and child protection. Beyond these general issues, several key points were raised, which the participants noted were worthy of further investigation.

Location-based services

Location-based services were top-of-mind for both freedom of expression advocates and child protection advocates. Most believed that while the services have largely remained uncontroversial to date, ignoring the technology until it becomes ubiquitous is a dangerous mistake. The market for location-based services is currently confused; some market the services to parents as a necessity for their children, while others market the service to adults and forbid its use by those under eighteen. Enforcement of these terms and conditions is inconsistent. Once again, transparency was advocated, with suggestions being made that these services be opt-in, clearly visible while in use, and transparent about how, when, and with whom information is being shared. Participants argued that companies should more clearly enforce terms and agreements for services that claim to be forbidden to minors. There was also general

(though not unanimous) agreement that forcing location-based services on children is a threat to their rights to privacy, autonomy, and dignity; children should always have the right to know that they are sharing their location, as well as the the right to turn off the sharing of that information. For guidance on the emerging discussion in this field, participants were directed to a recent report by John Carr for the European NGO Alliance on Child Online Safety, which outlines the history of the services and recommends a set of policy responses.[9]

Data Protection and Privacy

Location-based services were also mentioned as part of a larger set of data protection and privacy issues. It was generally agreed that children have the right to be free from covert monitoring, and that key loggers, screen shot recorders, or hidden audio or video surveillance by mobile phone should be discouraged in all or almost all situations. In cases where parents decide the use of these sorts of tools is necessary, they should discuss why with their children, inform them of their use, and obtain their permission. These services drew out the shared importance of data protection issues in general, especially as they concern mobile devices. Some freedom of expression advocates stressed that mobile and Internet service providers should gather only a minimum of data and only be required to keep it for a short period of time.

Liability of Internet Service Providers

Another emerging issue of interest to the group was the nature of liability for Internet service providers trying to reduce the risks for children on their networks or services. In most countries, ISPs enjoy immunity from prosecution for material belonging to users of their service as long as they act on illegal material brought to their attention. As a result, Internet services find a greater protection in law if they remain ignorant of the use of their services. The group was split on whether this approach should be encouraged, or whether services that actively police their networks to reduce risk for children should be assured that by doing so they would not lose their immunity in the case that something was overlooked. The practice of giving networks immunity from liability, if and only if they acted on actionable information, was also seen by some as a useful model for extending the responsibilities of service providers to policing their services for bullying and other inappropriate behaviour.

Other Emerging Issues

Several other emerging issues were identified by participants, including age verification for age-restricted products online, lawful interception legislation, the appropriate classification of written depictions and pseudo-images of sexual abuse, and the use of encryption. Time limitations meant that most of these issues remained unexplored during the course of discussion, but several of these issues are directly addressed in the position papers that accompany this report.

[9] http://www.chis.org.uk/2009/07/08/enacso-the-new-breed-of-location-services-july-2009

Where do we go now?

By meeting with open minds and a shared commitment to the protection of basic human rights, the participants of the Oxford Internet Institute's Forum on Child Protection and Freedom of Expression Online were successful in beginning a dialogue on finding common ground.

The day was designed not to craft policy, but to open channels of communication and map areas of agreement and difference. While most in the room agreed there was much more discussion to be had, we were largely successful in achieving our goals.

Making Good Policy

The day's biggest agreement was a simple one: 'If you're going to make policy, you'd better not make bad policy'. Further agreement was found on some measures of what makes good policy:

- Good policy is generic as opposed to technology-specific.
- Good policy uses clear and precise language.
- Good policy will hold up in court, and targets specific risks. It is born of real need instead of grandstanding.
- Good policy includes measurable goals and a commitment to following up, to ensure that the goals are being reached.

In order to influence good policy, it was agreed that there were opportunities for child protection and freedom of expression advocates to present a united front on some issues and that, to do so, the conversations started at the forum should be continued and expanded on.

It was also agreed that good policy should be informed by good research, and there was united support in encouraging governments to support more research. A similar call was made for public and commercial actors with active infrastructure to obtain the informed consent of their subjects and then share their data with researchers.

Participants in the forum will continue to pursue their agendas, and for each, the next steps may be different. For some, the next step is continuing empirical research; for others, the next step involves finding new ways of assessing risk and harm; and for others still, the next step is to look for ways to translate the agreements reached here into actionable advice to policy makers. After the forum's success in beginning a unique conversation between advocates, there remains significant scope for continuing the conversations begun at the forum.

References

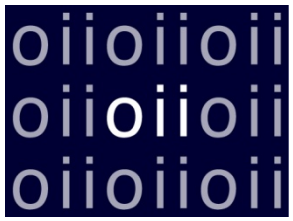
Rickert, V. I. and Ryan, O. (2007) Editorial: Is the Internet the Source? Journal of Adolescent Health 40: 104-105.

Wolak, J., Finkelhor, D., Mitchell, K. J. and Ybarra, M. L. (2008). Online "Predators" and Their Victims: Myths, Realities, and Implications for Prevention and Treatment. American Psychologist 63 (2) 111-128.

Hasebrink, U., Livingstone, S. and Haddon, L. (2008) EU Kids Online: Comparing children's online opportunities and risks across Europe. London: EU Kids Online.

Forum Participants

- Alison Powell (OII)
- Michael Hills (OII)
- Ian Brown (OII)
- John Carr (CCCIS)
- Zoe Hilton (NSPCC)
- Dieter Carsten (eNACSO)
- Ana-Luiza Rotta (eNACSO)
- Adam Thierer (Progress & Freedom Foundation)
- John Morris (Center for Democracy and Techonology)
- Leslie Harris (Center for Democracy and Techonology)
- Catherine Crump (ACLU)
- Lee Tien (EFF)
- Colin Jacobs (Electronic Frontiers Australia)
- Sonia Livingstone (London School of Economics)
- Geraldine von Bueren (Queen Mary, University of London; Visiting Fellow, Kellogg College, Oxford)
- Michelle Collins (NCMEC)
- Carolyn Atwell-Davis (NCMEC)



Oxford Internet Institute Policy Forum: Child Protection, Free Speech and the Internet: Mapping the Territory and Limitations of Common Ground

Participant Position Papers

Oxford Internet Institute

University of Oxford

2 October 2009

Position Paper of
Adam D. Thierer
(athierer@pff.org)
The Progress & Freedom Foundation
Washington, DC

Oxford University conference
"*Child Protection, Free Speech and the Internet*"

2nd October 2009

What is the nature of your interest or experience in this field?

I have spent the last 18 years covering the intersection of child safety concerns and free speech issues at four different think tanks. In recent years, I have tied together all my research in a constantly updated Progress & Freedom Foundation special report entitled, "Parental Controls & Online Child Protection: A Survey of Tools & Methods."[1] The 4th edition of this 250-page report was released in August.

Are there particular values or principles which underlie your work?

The goal of my research has been to explore the tension between free speech and child protection and to identify methods of striking a sensible balance between these two important values. It is my hope and belief that we are now in a position to more fully empower parents such that government regulation of content and communications will be increasingly unnecessary.

In the past, it was thought to be too difficult for families to enforce their own "household standard" for acceptable content. Thus, many believed government needed to step in and create a baseline "community standard" for the entire citizenry. Unfortunately, those "community standards" were quite amorphous and sometimes completely arbitrary when enforced through regulatory edicts. Worse yet, those regulatory standards treated all households as if they had the same tastes or values—which is clearly not the case in most pluralistic societies.

If it is the case that families now have the ability to effectively tailor media consumption and communications choices to their own preferences—that is, to craft their own "household standard"—then the regulatory equation can and should change. Regulation can no longer be premised on the supposed helplessness of households to deal with content flows if families have been empowered and educated to make content determinations for themselves. Luckily, that is the world we increasingly live in today. Parents have more tools and methods at their disposal to help them decide what constitutes acceptable media content in their homes and in the lives of their children.

Going forward, our goal should be to ensure that parents or guardians have (1) the *information* necessary to make informed decisions and (2) the *tools and methods* necessary to act upon that information. Optimally, those tools and methods would give them the ability to not only block objectionable materials, but also to more easily find content they feel is appropriate for their families. In my work, I refer to this as the "household empowerment vision."

Will we ever be able to achieve a world of *perfect* parental control over all online content and communications? That is unlikely since both content and technology will continuously evolve and make that goal elusive. But government regulation of speech should yield where less

---

[1] Adam Thierer, The Progress & Freedom Foundation, *Parental Controls and Online Child Protection: A Survey of Tools and Methods*, Special Report, Version 4.0, Summer 2009, www.pff.org/parentalcontrols

restrictive alternatives such as household-based controls and strategies exist. Given the value associated with free speech and the danger of government censorship, these alternatives need not be perfect to be preferable to government regulation.

What are the issues/policies or laws which you see as most problematic in terms of creating or illustrating a conflict between online child protection and free speech?

It is essential that policymakers resist the temptation to extend traditional broadcast industry regulatory statutes and standards to new media outlets and digital technologies. In a world of media convergence and increasing user empowerment, traditional regulatory rationales make increasingly less sense. Nonetheless, many ongoing social problems and challenges remain to achieving the "household empowerment vision" I outlined above, including:

- **The "lack of awareness" problem:** Some parents remain unaware of empowerment tools.
- **The "bad parent" problem:** Some parents don't use tools even when aware of them.
- **The "bad neighbor" problem**: "Good" parents fear what happens when their kids visit other kids with more permissive parents.
- **The "generation gap" problem**: Kids sometimes know more about new digital technologies than their parents.
- **The "technological surprise" problem**: Rapid emergence and diffusion of new digital technologies can catch some parents by surprise.
- **The "bad corporate actor" problem**: Most companies self-regulate, but a handful push the boundaries of good taste in ways that create social concerns that reflect on industry generally.
- **The "user-generated content" problem**: Even when "professional" content can be managed, it is difficult to control "amateur" expression and creations.
- **The "peer-on-peer bullying" problem**: While many are concerned about predators, the real online safety problem turns out to be cyber-bullying among peers.

Because of these ongoing social challenges or concerns, legal and regulatory proposals will continue to be put forward. But each has serious downsides:

- **Future of filtering:** Centralized, network-based or decentralized, user-based? The former creates serious censorship threats, as we see in China and other repressive states. The latter is more consistent with the household empowerment vision.
- **Middleman deputization:** Should online intermediaries be required to police the Net for various social ills? If so, as hand-maidens of the state, they could become over-zealous speech regulators.
- **Universal content ratings:** Can policymakers mandate unified (or "scientific") content media ratings? Doing so puts regulators in a position to dictate content standards—for better or worse. Moreover, this does nothing to address user-generated "amateur" content.
- **Mandatory online age / identity verification:** Potentially threatens anonymity, privacy, and free speech rights. Moreover, to the extent "bad guys" continue to get into "secured" environments it creates a false sense of security for parents and kids.

- **Expanded data retention:** Although it would help facilitate some law enforcement goals, it also gives rise to new privacy and data breach risks.

Might any of these conflicts be avoidable, e.g. through the use of improved legislative instruments or greater clarity and accountability in processes of self-regulation?

For the above reasons, it makes more sense to put our energies into finding new self-regulatory mechanisms, social norms, and user empowerment strategies to solve ongoing social problems instead of focusing on regulatory solutions or mandates. Instead of providing greater clarity, legislative instruments are more likely to instead create greater ambiguity, or at least uncertainty, for content creators and consumers alike. This is because, as was noted above, "community standards" are notoriously subjective; they are ham-handed attempts to gloss over the diverse needs and values of a diverse citizenry. By contrast, self-regulation, social norms, and empowerment strategies are evolutionary in character and more responsive to differences among cultures and households.

What are the issues where you think there might be most scope for finding some common ground?

In two words: *empowerment* and *education.* Because reliance on legislation is perilously difficult and enforcement of regulatory mandates is complicated (and sometimes impossible in an increasingly borderless world), efforts to better empower families and educate both kids and parents offer the most sensible path forward. All stakeholders involved in child safety and free speech debates can generally agree that empowerment efforts, media literacy programs, awareness-building programs, and so on, are both effective and unobjectionable.

At the international level, are there certain key principles which we ought to be defending above all others?

Because of the "values clash" at the international level, it's hard to imagine we'll ever achieve consensus on some of these issues. Countries vary widely in their sensitivities about speech, making any attempt to devise "universal principles" complicated. For example, Europeans generally deride America's prudish ways when it comes to matters of sexuality or "indecency." By contrast, most Americans cannot understand European concerns about "hate speech" or violently-themed media. Meanwhile, governments in many other parts of the world are still busy trying to quell political or religious dissent. "Harmonization" among those competing cultural norms remains complicated, therefore, and it would be a mistake if international harmonization was accomplished by sacrificing free speech rights for countries and cultures who cherish them.

"Child Protection, Free Speech and the Internet"
Oxford Internet Institute, 2nd October, 2009

Outline Paper for Discussion

John Carr
Dr Zoë Hilton

1. Nature of interest

We are child protection advocates working for independent, professional not-for-profit child protection and child welfare agencies that engage with a broad spectrum of issues concerning children. Some of our agencies are very substantial household names, dating back to the mid-19th century and employing upwards of 6,000 full time employees.

2. Broad principles

The core document which underpins our work is the UN Convention on the Rights of the Child. Inter alia, this asserts that children have a right to grow up free from a variety of forms of exploitation and that states have an obligation to uphold and provide for that right. A child is any person under the age of 18, but the Convention stresses the need to be alive to the evolving capacities of the child i.e. one's obligations to a child of three are not the same as one's obligations to a person of 17.

3. Problematic areas

The role of state

In our view the state is the child protection agency and child welfare agency of last resort. It is of course highly preferable that parents and families take the lion's share of the responsibility for children's upbringing, and that includes teaching about and making provision for the safe use of the internet, but the key point is the state can never absolve itself of any or ultimate responsibility. Parents, families, schools and other social institutions are not at liberty to harm their own or anyone else's children, either by acts of omission or commission. Self regulation is simply a pragmatic response to the new complexities facing most governments. It is not an eternal principle.

Children's interests never considered

We entirely support the core principles of declarations such as, for example, the Global Network Initiative. However they frequently appear to be based on the unspoken assumption that the internet is entirely populated and used solely by adults with full legal capacities. No one wants an internet that is only fit for children but equally no one should want an internet where children's large scale presence is discounted or ignored.

The role of technical measures

As children's organizations we have no desire to see child protection used as a smokescreen to justify wider forms of censorship, repression of free speech, particularly in the political arena or in areas connected with artistic expression. However, as with many other public spaces, there is a proper role for interventions which seek to guarantee or maintain their integrity. In the case of the internet that inevitably introduces a consideration of the role of filtering products. We do not see that where minor barriers or inconveniences are erected or contrived to protect the unwary, the ignorant or the unqualified, as they are in real life, that this amounts to "censorship".

Turning to the specific questions asked by the OII

4. **Child abuse images**.

The arrival of the internet has completely transformed "the market" for child abuse images. It has become a "signature" crime of the internet.

Institutions such as hotlines can provide an enormously valuable way of dealing with child abuse images. The basis on which they are constituted and on which they act must be transparent. It should not be possible for anyone to harbour any reasonable suspicion that a hotline is capable of being used to block or remove any other kind of material. It should be clear that when a hotline acts it is acting in a quasi-judicial capacity and their actions are therefore potentially subject to judicial review.

The use of block lists should be encouraged. In the UK it is a crime both to advertise the availability of child abuse images and to supply them. Thus Usenet Newsgroups which do either or both are de-listed. Web pages or, if appropriate, entire web sites, containing illegal images are put on to a database and access to them is denied.

It is important to be practical in relation to these challenges. It would be absurd, for example, for every image to be viewed by a judge before it could be made the subject of a take down notice. However the UK approach should be contrasted with others that can cause "collateral damage" to wholly innocent web sites which have the misfortune to find they are sharing a domain name or an IP address with some illegal content.

5. **Pseudo images**

In several countries the only basis on which an image can be deemed to be capable of being classified as an illegal child abuse image is if it depicts actual harm being done to a real child. Bearing in mind that by definition a pseudo image must be indistinguishable from the real thing, we can see no proper basis for making such a distinction. If as a matter of fact an

image looks as if it is showing a real child being harmed in a real way then it should be treated as being exactly that without the need for more.

6. **The role of filtering products**

Too much of the present discussion about filtering is essentially about minimising the potential cost or inconvenience to companies or it is to do with alleged worries about the impact on network performance. These are not unimportant issues but they ought not to be elevated to a supposed principle.

Where internet enabled devices are being sold into the consumer space they should come with child safety software preinstalled and preconfigured. There should be full transparency as to the basis on which the filters work. Families should of course be free to vary the settings in whichever way they choose, or indeed to abandon such software altogether but the current situation is based on a fiction. Families should not have to jump through hoops to make a device as safe as it can be from a technical perspective.

Technology companies deploy a host of technical measures to try to pre-empt criminal, damaging or other incidences which they judge to be undesirable and which breach their T's& C's. Many of these work at network level and are not presented or advertised as consumer choices e.g. most networks filter out spam by default, even though this does occasionally mean that an end user might miss or lose a legitimate email. In relation to dealing with illegal content we can see no coherent case for not filtering at network level. Everyone has a responsibility to deal with illegal content.

7. **Children's right to access information**

In the UK, children's rights to access information are, in principle, identical to those of adults. However children do not have a legal right to opt to harm themselves and the law says they are not always going to be fully competent to decide what is in their own best interests. Adults and companies therefore have an obligation to use their best judgment about what is in the interests of a child and this must take account of what is in the interests of that individual child. Again, transparency is paramount.

8. **Data privacy**

In the UK children's rights to privacy are again, in principle, identical to those of adults but in the end everything hinges on the individual capacity of a particular child to understand the nature of the transaction being put to them i.e. it is a subjective test. No one has ever explained how such a test might be carried out in a remote environment such as the internet. For that reason, at least for the time being and only in relation to remote environments, we favour the introduction of something like COPPA.

9. **Age verification**

The internet should not become a way for vendors to avoid being caught by laws which limit the age at which a range of products or services can be supplied to minors e.g. tobacco, alcohol, weapons, pornography and gambling. To that extent, persons wishing to buy such things online must accept that they have to prove they are legally qualified to do so. Beyond that we broadly concur with the findings of the ISTFF in relation to age verification and social networking sites.

10. **Encryption**

This is perhaps one of the most challenging areas. The police and ISPs are reporting a steady rise in its use. It is increasingly frequently turning up in environments which very clearly suggest it is being used for criminal purposes or to hide the evidence of crimes e.g. against children. The right not to self-incriminate needs to be re-examined in the light of the emergence of strong encryption. With appropriate judicial oversight we favour the creation of an obligation to provide decryption keys to establish whether or not material relevant to the investigation of a crime is being hidden.

---ooo---

"Child Protection, Free Speech and the Internet"
Oxford Internet Institute, 2nd October, 2009

Discussion points

Dieter Carstensen
Save the Children Denmark / eNACSO (The European NGO Alliance for Child Safety Online)

Save the Children (SC) is the largest independent children's rights organization consisting of members in 29 nations throughout the world. SC has been operative since 1919, celebrating its 90th anniversary this year. The European members of the International alliance have a particular focus on child online protection and safety, and we have been operative in this specific area very much since the **1996 Stockholm First World Congress against Commercial Sexual Exploitation of Children.**

SC members are operating a variety of initiatives from awareness raising over education to combating online related sexual abuse of children.

All SC members are operating under the mandate of the UN Convention of the Rights of the Child, the most important and significant tool in the defence and promotion of children's and adolescents' rights. Relevant for this discussion is in particular the Conventions

- Article 13 highlighting the child's right to freedom of expression (as well as the restrictions that might apply),
- Article 16 highlighting the child's right to privacy and the protection of this,
- Article 17 regarding access to information of social and cultural benefit to the child as well as the protection from information and material injurious to his or her well-being,
- Article 34 highlighting the duty of states to take all appropriate measures to prevent the exploitative use of children in pornographic performances and materials

The issues

The emergence of proactive blocking of access to websites with content deemed, by relevant institutions, to contain child sexual abuse material, has been the major area of conflict in the public debate. Whereas from a child protection perspective, the need to protect the child and the reputation of a child is a key element of our operations, the blocking methods implemented has a potential for collateral damage, like over-blocking as well as using the blocking of child abuse material initiative to cover more than the stated.

A child who has been subject to abuse and had the abuse documented and consequently digitalized and uploaded will always be aware of the existence of such material. Hence, the need for the society to reestablish and protect the dignity of a child victim is important. Where such material is available, identified and classified, appropriate steps to hinder its further distribution and dissemination must be taken by all relevant parties. The technique of blocking content has in principle a notion of censorship, but by limiting its focus to solely cover the aforementioned type

of material, it is moreover a question of fulfilling a child's right to protection from re-victimization. In addition, it provides hope to the child of restoring its dignity and reputation. A further note that is relevant is the proposed "EU Framework Decision on combating the sexual abuse, sexual exploitation of children and child pornography" where steps to hinder access to known child sexual abuse web content must be taken by member states. Blocking is one of such measures.

Needs

In regards to content blocking, a noteworthy trend (as seen in Germany and in South Korea) is to have an independent board of reviewers who will assess the list of websites that are to be blocked. The review board will have experts from different fields of knowledge so to be able to balance the decision making justly across interests and backgrounds. By having such a review board ascertaining that the list exclusively covers child abuse material, the opposition who states their distrust in blocking can be reassured. In essence, providing greater transparency to content blocking is a required further step to take.

Child sexual abuse material

The variety of measures taken to help the fight in eradicating online child sexual abuse material are all part of a greater puzzle, a wider approach. This wider approach operates more holistically where awareness, education and empowerment are cornerstones in the child's upbringing and preparation for encountering the world of their peers as well as the one of the grown-ups. However, all measures henceforth implemented are coming short in reaching and having the desired effect on all children, hence, you will always have a more vulnerable child or young person who is inclined to take greater risks and possibly even provoke illegal behavior. Some of these incidents are resulting in the documentation of the abuse, the criminal act, and as such, the society as a whole should act appropriately and determined to rectify this.

There are many child abuse images which are realistic images of a non-existing child engaged in sexual conduct, or 'pseudo images'. These include non-photographic visual depictions of child sexual abuse (i.e. computer generated images (CGIs), drawings, animation) as well as 'pseudo-photos' or videos. In our experience this type of material has clear risks insofar as it can form part of a subculture of sexual abuse material and if it is not criminalized the police are not able to seize the materials or disrupt the network of traders. The existence of such materials allows offenders to deny and minimize the impact of sexual abuse and encourages distorted thinking about sexual crimes against children. Furthermore, there is evidence to support the fact that photographs of children engaged in sexual activity are used for grooming children into child pornography, and that pseudo-photographs will also be used for this purpose. Thus, all states should ensure that pseudo images are made illegal.

Filtering products

The nature of cultural differences and contexts requires an equally targeted response when discussing filtering mechanisms. If we assume that filtering tools are aimed at increasing the likelihood of 'safer surfing' by children, then it can be argued that all internet enabled devices should be equipped with filtering tools, and preconfigured to the highest safety standard, accompanied with easy to use instructions to the guardian / parent on how to adapt the settings so to better match the individual family members needs and ability. By enforcing this approach, we

will allow for children with lesser involved or informed parents /guardians to access the internet with the best possible measure for safeguarding them from harmful content and contact. However, as with all technical solutions, it is one piece of the puzzle in a necessary multi-pronged approach. It needs to be accompanied with relevant educational awareness material.

Access to information

As stated in the CRC's Art. 17, every child has the right to obtain access to information. However, the restriction imposed on them vis-à-vis usage of filtering, white lists etc can rightfully be justified in the context of protecting them from harmful content and other content not appropriate to their age.

Electronic Frontiers AUSTRALIA

Child Protection, Free Speech and the Internet
EFA Position Paper

1. About Electronic Frontiers Australia

Electronic Frontiers Australia Inc. (EFA) is a non-profit national organisation representing Australian Internet users concerned with on-line freedoms and rights. EFA was established in January 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's activities include public outreach and media liaison, direct lobbying of politicians and political parties, submissions to law reform and parliamentary committees.

2. Key Points

There is increasing worry in the community, both in Australia and around the world, about the safety of children online. The easy availability of adult content, high-profile busts of pedophile rings, and sensational stories of chat-room predators lead many to the conclusion that the Internet is a dangerous place for minors to inhabit. At the same time, today's youth have grown up in a wired world, and spend much of their time online, further increasing parental concern.

Lawmakers, whether sharing the concern or seeking to profit from it, have from time to time made various proposals to mitigate the perceived risks to children. These frequently include calls to regulate Internet content via the means of classification and/or censorship. This ranges from forcing public libraries and government agencies to install commercial filtering software to national or ISP-level programs to restrict access to prohibited content in real time.

In general, these schemes are impractical, provide few tangible benefits for children, and unnecessarily encroach on citizens rights to freedom of communication and expression.

3. Internet Censorship in Australia

i. History and current situation

A 1999 push by the Australian government to prohibit certain types of online content eventually resulted in a system where the media regulatory body, the Australian Communications and Media Authority, receive and process complaints from the public about Internet content. If a web page is deemed to contain "prohibited content" - content that would be restricted to adults or banned in other formats[1] - it is either a) to be removed by the web host, under threat of sanctions, if hosted within Australia, or b) added to a blacklist to be provided to the manufacturers of PC filters. (Australian ISPs are required to make such filters available to their customers.)

In addition, the previous government funded a scheme called "NetAlert" in which PC filtering software was made available, free of charge, to all Australian users, and provided with technical support at government expense. Due to low rates of adoption by the public, this scheme was terminated by the current government.

ii. Current Proposal

The Australian Labor Party went to the last election with a comprehensive plan for "cyber-safety" - that is, making the Internet safer for children. The centrepiece of this policy, and its most expensive component, is the controversial national ISP Internet filtering scheme. The filter is designed, in theory, to protect children by shielding them from age-inappropriate online content, and by preventing the spread of child-abuse material online. If this plan is implemented, Australian Internet users will find themselves part of a two-tier system. The first tier, which is to be mandatory for all Australians, will involve a government-controlled blacklist of prohibited sites that ISPs must block. The second tier, which Australians may opt-out of, involves a more aggressive filter that is to remove all material "inappropriate" for children. (It should be noted that only the second, optional filter was presented to the public before the election. The mandatory filter, along with the new censorship powers behind it, was not an election promise.)

Despite its stated rationale of protecting children, the policy has been very controversial. Opponents don't dispute the worth of this goal, but take issue with the expense, side-effects and ineffectiveness of the scheme. Those criticising the filter include ISPs concerned about the technical problems and costs, civil-libertarians worried about the process of censoring internet content, and analysts concerned at the expense and ill-defined policy goals.

4. Child Protection and Child Rights

Without question, children have a need and a right to be protected from harm, and such concerns deserve serious consideration at a policy level. Regarding the risks children face online, EFA contends that much discussion - and policymaking - in this arena is based more on gut feelings about the nasty corners of the World Wide Web and less on real research that quantifies the actual risks and harm. The enormous benefits minors reap from online interactions are also seldom discussed.

A recent report by Harvard University concludes that the risks to children are, in general, overblown. On the subject of inappropriate material, the study's authors conclude that "the Internet increases the availability of harmful, problematic and illegal content, but does not always increase minors' exposure. Unwanted exposure to pornography does occur online, but those most likely to be exposed are those seeking it out, such as older male minors."[2] Because of the ever-changing nature of web content and the ease with which filters are bypassed, an ISP level filter is unlikely to prevent those who are determined to find such material from accessing it.

More significant risks include cyber-bullying, and other interactions with peers and others online. This also must also be put in perspective, as online interactions are only a subset of a child's social interactions - that is to say, cyber-bullying is only a part of a larger issue of bullying in general, perpetrated against the same children by the same peers.[3] In any case, these issues are not amenable to a technical solution.

While striving to protect children, the children's rights must also be taken into account. For instance, Holly Doel-Mackaway, a child rights advisor for Save the Children Australia, has opposed the filtering policy not only as a waste of resources, but as contrary to the rights of children to access helpful and developmental information which could be blocked. [4]

The production and dissemination of child sexual abuse material is also of clear concern in terms of child protection. Blocking access to such material is potentially more feasible than rendering the entire world of web content “child-friendly”. Practically speaking, however, such material is seldom trafficked on the public internet.[5] Attempts to block access to such material would be easily circumvented by those determined to access it. On the other hand, law-abiding internet users and taxpayers would have to support the implementation of a scheme to censor their Internet access with a blacklist that must, by its nature, remain secret and unaccountable. EFA feels that law enforcement is a more effective and transparent way to combat such material.

5. Conclusion

Children face real risks online. These risks include cyber-bullying, the theft or dissemination of personal information, and exposure to harmful content. It is natural that both as parents and as a society that we wish to do everything possible to minimise those risks. However, it is important to take an evidence-based approach weigh the costs of proposed measures against the real benefits for children.

What we find is that proposals to restrict access to information online at the national level are amongst the first remedies proposed but are also the most expensive, democratically fraught and technically complex. While such a scheme would theoretically reduce the exposure of children to inappropriate content, we find that firstly, filtering out all such content (especially when maintaining access to this content by adult users) is impossible, and secondly, exposure to unwanted content, while it does occur, is among the least significant risks children face online.

Given the real conflict between mandatory Internet censorship and the right to freedom of speech taken for granted in most democratic countries, it’s hard to imagine a situation in which such a censorship scheme could be supported, let alone on child-safety grounds.

That doesn’t mean we have to disagree with those campaigning on behalf of children. The real risks can be accurately quantified and addressed. Firstly, we advocate more study be undertaken so that the facts can be better understood, including the risks children themselves identify as the most significant. Secondly, education must be a central part of any plan to address cyber-safety. Parents and educators must be made aware of the challenges children face online and how best to tackle them, including technical solutions such as filters in the homes where necessary.

Finally, we advocate maintaining a well-resourced police force who can tackle the production and distribution of child abuse material in the most appropriate way - as a serious criminal enterprise, not a technical problem.

---

[1] http://www.acma.gov.au/WEB/STANDARD/pc=PC_90102

[2] Berkman Center for Internet and Society at Harvard University, *Enhancing Child Safety & Online Technologies: Final Report of the Internet Safety Technical Task Force*, p. 5.

[3] Studies indicate almost all cyberbullying is conducted by other youth, and these are mostly known to the victims. See Berkman, p. 17.

[4] http://www.onlineopinion.com.au/view.asp?article=8445

[5] http://www.schneier.com/blog/archives/2009/03/the_techniques.html

Further Reading:

About EFA:

http://www.efa.org.au/about/

About Cyber-safety:

The Internet Safety Technical Task Force, Enhancing Child Safety and Online Technologies Final Report: http://cyber.law.harvard.edu/pubrelease/isttf/

Review of Existing Australian and International Cyber-Safety Research, Child Health Promotion Research Centre Edith Cowan University, May 2009 http://tinyurl.com/noadst

Internet Industry Association Feasibility Study - ISP Level Content Filtering: http://www.dbcde.gov.au/funding_and_programs/cybersafety_plan/internet_service_provider_isp_filtering

About illegal material:

Irene Graham, Statistics Laundering: false and fantastic figures: http://libertus.net/censor/resources/statistics-laundering.html

About the censorship debate in Australia:

Derek E. Bambauer, Brooklyn Law School: *Filtering in Oz: Australia's Foray into Internet Censorship* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1319466

EFA Filtering Fact Sheets: http://www.efa.org.au/mandatory-internet-filtering-fact-sheets/
Overviews of current plan: http://www.efa.org.au/censorship/mandatory-isp-blocking/
http://libertus.net/censor/ispfiltering-au-govplan.html

Opinion:
http://www.theaustralian.news.com.au/story/0,25197,26018290-7583,00.html
http://www.efa.org.au/2009/01/14/filtering-wont-deliver-for-aussie-kids/
http://www.efa.org.au/2009/02/20/cyber-libertarians-love-their-children-too/

Position Paper of the

Center for Democracy & Technology

Leslie Harris, President
John Morris, General Counsel

1634 I Street, NW Suite 1100
Washington, DC 20006
202.637.9800
fax 202.637.0968
http://www.cdt.org

Prepared for the conference on
"Child Protection, Free Speech and the Internet"
hosted by the Oxford Internet Institute

October 2, 2009

The Center for Democracy & Technology ("CDT") appreciates the opportunity to participate in the Oxford Internet Institute's conference on Child Protection, Free Speech and the Internet. We believe that both child protection and the protection of free speech rights are critical goals in our society, and that there is strong potential for cooperation and mutual understanding among groups pursuing each of these goals.

• What is the nature of your interest or experience in this field?

CDT is a non-profit public interest and Internet policy organization dedicated to preserving and promoting openness, innovation, and freedom on the decentralized Internet. In particular, CDT works to protect freedom of expression online, including the right to speak anonymously and to engage in robust communication free of unconstitutional or inappropriate restrictions on the ability to convey and access lawful content.

CDT has been a leader in the effort to protect and promote freedom of expression on the Internet. It helped to organize one of the legal challenges in 1996-1997 to the "Communications Decency Act," a case in which the U.S. Supreme Court established that speech on the Internet receives the highest level of protection under the First Amendment of the U.S. Constitution. More recently, CDT successfully challenged a state law in Pennsylvania that – although well-intended – did almost nothing to fight child pornography (the law's intended target) but simultaneously led to the blocking of access to more than 1.5 million unrelated and wholly lawful web sites. (John Morris was a lead counsel in both of these cases on CDT's behalf.)

As a critical compliment to its free expression work, CDT has been a strong and very early advocate for the "user and parental empowerment" approach to child protection, urging that parents should have robust tools available to them so that they can make personal decisions about what content their children can access. From as early as 1995, CDT has presented to policy makers, legislators, and the courts evidence about how user empowerment tools work, and how they can be more effective (and less invasive) than direct government regulation of online content. We also believe that education – of both children and parents – is an essential element of any effective effort to promote online child safety.

CDT has over the years participated in a number of task forces and working groups focused on online child safety. Most recently, CDT served on the Internet Safety Technical Task Force, which studied the nature and extent of child safety threats online and examined tools and strategies

available to parents to help keep minors safe online. CDT currently is a member of the Online Safety and Technical Working Group created by the U.S. Congress to study online child safety.

• Are there particular values or principles (ethical, legal or constitutional) which underlie your work?

CDT works on the full range of public policy issues relating to technology and the Internet, and promotes a range of values such as privacy, free speech, network neutrality, and open government. A number of particular values are of direct relevance to the conference:

1. Free speech as protected by the First Amendment of the U.S. Constitution is a fundamental principle to CDT. The First Amendment holds a unique and critical position in America's very identity – the desire to be free from government censorship was one of the key motivating goals in the American Revolution that led to the founding of our country. The First Amendment is one of the most important and overriding principles of the U.S. constitutional and governmental system. The First Amendment is a powerful bar against governmentally-imposed regulation of speech, except in the narrowest of circumstances and subject to exacting "due process" procedural requirements. At times, the First Amendment can lead to some social wrongs being left unpunished in the name of protecting broader rights to free speech.

2. Particular aspects of First Amendment jurisprudence are also important principles that CDT works to protect. For example, we strongly support the right to speak and receive information anonymously, including the right to access publicly available content on the Internet and interact with other Internet users without identifying oneself. Although the right to anonymity is not absolute, it is an important First Amendment value.

3. Similarly, the rights of minors to create and receive speech online is protected by the First Amendment, and we strongly believe that such rights should be upheld and defended. Indeed, in some contexts we believe that a minor has rights to access content even where such access runs counter to the parents' wishes.

4. Child safety is also a very important value to CDT, and we work hard to promote (in the U.S. Congress and elsewhere) solutions that promote child safety in a manner that respects our constitutional rights and free speech values. Too often online child safety proposals in U.S. legislatures are based on simplistic or flawed assumptions, and do not address the root of the risks.

• What are the issues/policies or laws which you see as most problematic in terms of creating or illustrating a conflict between online child protection and free speech?

The Internet has been so transformative in our society because it is so open, such that anyone can publish, speak, and reach the entire world at a very low cost, and anyone can innovate and create new technologies and services without seeking permission of a government or service provider. This openness and accessibility is what sets the Internet apart from every other form of media that has ever existed.

But this openness also means that those who might create risk for children can also be online. The fundamental challenge of child protection efforts is to protect children and promote online safety while still preserving the openness and innovation that are critical to the Internet.

One tremendous difficulty is that legislators sometimes perceive – incorrectly – that intermediaries such as ISPs and other service providers provide a quick and easy avenue through which to address a social problem such as child safety. The architecture and technical characteristics of the Internet, however, can make that approach very problematic, and often ineffective as well.

• Might any of these conflicts be avoidable, e.g. through the use of improved legislative instruments or greater clarity and accountability in processes of self-regulation?

These tensions can be reduced by focusing legislative efforts on bolstering law enforcement resources to identify and prosecute the actual perpetrators of crimes against children. Governments could also strengthen such legislative strategies by supplementing vigorous prosecution with additional support for user empowerment/parental control tools and educational resources for both guardians and children. Legislation seeking to make intermediaries the "traffic cops" of the Internet will encounter substantial technical obstacles and – in the U.S. – significant constitutional barriers.

Voluntary efforts by industry participants can also be valuable, so long as they are truly voluntary (and not the product of a government seeking to achieve through coercion and threat what is cannot permissibly do itself) and respect the rights of users to publish and access lawful speech.

• What are the issues where you think there might be most scope for finding some common ground?

We all share a strong believe in protecting children, and we hope that we all share an equally strong belief in protecting civil rights and liberties. It is vital that, in promoting online child safety, we at the same time respect the legal and constitutional principles on which our society is based.

We will likely find the most common ground on the goal of supporting law enforcement efforts to prosecute those who commit crimes against children, and on the right of parents to guide their children's access to online content.

• At the international level, are there certain key principles which we ought to be defending above all others?

Among the key principles that we should all embrace are:

- The Internet has tremendous value and benefits for young people.
- Crimes against children should be vigorously prosecuted.
- Nations should cooperate in the investigation and prosecution of crimes against children that take place internationally.
- The right of freedom of expression must be honored: no nation should seek to impose domestically-acceptable speech restrictions outside of its borders, thereby seeking to impose its values on citizens of countries with differing values.

We look forward to the conference and dialogue on the critical issues of child safety and free expression, and to exploring where we stand on common ground.

Child Protection, Free Speech and the Internet: Mapping the Territory and Limitations of Common Ground

Paper for Discussion
Ana Luiza Rotta Soares
Project Director
PROTEGELES

Nature of the interest

I am a child protection advocate working in a non-profit, independent organization that runs the Spanish hotline and the Spanish awareness center funded under the European Commission's Safer Internet Programme[1].

Our organization firmly believes that the Internet and interactive technologies in general offer endless possibilities to children and adolescents to communicate obtain information and express themselves, using creativity and imagination. Positive Internet content promotes these positive behaviors.

Nonetheless, one of our core motivations is the eradication of child sexual abuse images from the Internet. Child Pornography (term used in the Spanish Penal Code) is illegal in Spain and we work closely with the Spanish National Police and the Guardia Civil reporting these sites.

Furthermore, our organization carries out awareness campaigns directed at improving the safety of children and young people in the use of interactive technologies. I am also a member of ENACSO (the European NGO Alliance for Child Safety Online) a network consisting of children's rights NGOs from across the EU working for a safer online environment for children.

Values/Principles

My work and that of my organization is guided by the UN Convention on the Rights of the Child. In adopting the Convention, the international community recognized that people under 18 years of age often need special care and protection that adults do not.

We are specially focused on Articles 34 and 35 of the Convention which state that governments should protect children from all forms of sexual exploitation and abuse and take all measures possible to ensure that they are not abducted, sold or trafficked. Our work also follows the principles set forth in the Convention's Optional Protocol on the sale of children, child prostitution and child pornography. The Protocol provides States with detailed requirements to end the sexual exploitation and abuse of children. It also protects children from being sold for non-sexual purposes—such as other forms of forced labour, illegal adoption and organ donation.

In addition, regarding the access to interactive technologies by children, we believe that the Internet and online technologies in general are essential to guarantee the implementation of Article 17 of the Convention that asserts that state parties must ensure that the "child has access to information and material from a diversity of national and international sources, especially those aimed at the promotion of his or her social, spiritual and moral well-being and physical and mental health". However, we believe that there is still a long way to go in order to guarantee an Internet that respects and considers the rights of children.

[1] http://ec.europa.eu/information_society/activities/sip/index_en.htm

Conflictive Issues

Sharing responsibility

Our experience in this field in the past decade has shown the need for a collaborative approach both at the national as well as the international levels regarding child protection in the use of interactive technologies. A multi-stakeholder approach is crucial both in the elaboration of supportive research as well as in the planning and implementation of campaigns. Stakeholders at all levels (governments, industry, parents, schools, parents and teachers organizations, children and adolescents, law enforcement, the media, child welfare organizations, etc) need to recognize that the protection and education of our children in the safe and responsible use of online technologies is NOT SOLELY the job of the parents, the schools or the governments. All stakeholders have a role to play in managing potential risks to children and adolescents. Industry, NGOs, governments, parents and teachers groups, research centers, etc need to work together, consulting and collaborating with each other in order to generate a culture of net-citizenship among youngsters.

In addition, we have to understand that not all parents and families are always looking out for the benefit of their children. Studies have shown over the years that most cases of child abuse occur within the family. Children that are exposed to abuse and violence within their families need also to be taken into consideration. They should have access to information and materials that will provide them with full and positive experiences with online technologies. Besides that, they should be given instruments to report and to seek help whenever necessary.

Child pornography

Internet and online technologies have been key for the dissemination and organization of groups that promote and commercialize with child abuse. Pedophilia has been a reality since the beginning of times, however the Internet offers pedophiles channels of communication and association never before imagined.

Images of children being raped and abused on the Internet are ILLEGAL and under no circumstance should be circulating the Internet. The production, distribution and consumption of these types of images should never be safeguarded by free speech legislation. However, a great deal still needs to be done in order to give the problem of pedophilia and sexual abuse of children the gravity required. These issues demand much more sensitivity on behalf of legislators, more resources for the Police carrying out investigations, more preventive work, more control over offenders and more attention to the children who are victims, etc.

Initiatives, such as hotlines, should be supported. However, their work needs to be transparent. Users need to know at all times and without a doubt what a hotline is fighting against, be it child pornography, racism, pro-anorexia pages, etc. In addition, initiatives should be backed by a solid group of stakeholders in their country that should include: law enforcement, government, child welfare organizations and industry. Staff needs to be carefully vetted in order to deal with such sensitive material.

Furthermore, we have been firm supporters of the use of blocking through the creation of blacklists that are distributed to ISPs for filtering child sexual abuse images. In Spain the process is well advanced and it is being led by the Spanish National Police and Guardia Civil. In our country's context, we believe that lists should be assembled and distributed by Law Enforcement Agencies since it is a way to ensure that ISPs are motivated to adhere to the project. However, we have always defended that users should be informed of the reason a determined page was blocked when the system is functioning. This guarantees greater transparency to the whole process.

Additionally, we fully support initiatives such as the European Financial Coalition against child sexual abuse images. However, we believe that eradicating commercial child sexual abuse images will only solve part of the problem. More effort needs to be placed in eradicating "home-made" non-commercial child sexual abuse images being distributed on the Internet. At our hotline, for example, most of the content reported to us refers to non-commercial child pornography (around 90% of the reports we receive). Therefore, we believe that non-commercial child pornography is a real problem that needs further study and actions.

Written and pseudo child pornography

Pseudo child pornography and morphed images are illegal in Spain already. However, we are currently working to raise awareness for the illegalization of written child pornography. Our organization has carried out a study on forums that eulogize pedophilia. These forums have become the "legal" points of contact and meeting for pedophiles all over the world. Many forums do not contain illegal images, but they are the place from which pedophiles come in contact, exchange emails and afterwards exchange illegal material. The texts presented, often disguised as "testimonies of readers", always have the same goal: to justify, defend and normalize pedophilia, including relationships with children of all ages who have no legal capacity to consent. They justify the sexual abuse of minors. In our study we found some comics that said things like "all men have that fantasy but suppress for fear of the police," for example.

In addition, we believe that these forums promote the abuse on children. Their stories and texts have a strong pornographic content, that is, they also seek to stimulate the reader. The brain is the main organ involved in sexual stimulation. No images are necessary for this stimulation. That is why today we can find certain pornographic magazines containing 75% of text and only 25% of images. We live in the world of supply and demand. These forums promote the development of demand: demand for child pornography and child prostitution. Satisfying these demands is a crime. Therefore, these forums encourage criminal activity and behavior. The same way that Europe is criminalizing the eulogy of racism and xenophobia, as well as the glorification of terrorism, we believe it would be reasonable and congruent to criminalize the eulogy of pedophilia, or what is called in Spain WRITTEN CHILD PORNOGRAPHY.

Filtering Software

As a principle, we believe that the first and utmost important rule in order to protect children from harmful Internet content is dialogue. Parents should listen to their children and talk to them about potential risks regarding the use of new technologies. We encourage parents to make the use of the Internet a family activity, to navigate with their children and to find out where they go and what they do, showing interest and respect for them.

With all of that in mind, our organization fully supports the use of filtering systems in families in order to regulate the navigation of children and to guarantee a positive experience on the Internet. We believe that filtering systems are the most effective barrier between children and content easily available on the Internet that might be harmful for their full development. Filtering systems, when used appropriately, empower parents and families, allowing them to determine exactly what should and should not enter their homes. We ask from filtering companies to develop more systems that enable parents to determine the different settings for the protection in their own homes, making the parents active participants in their family's safety and at the same time respecting cultural and educational differences present in each family. For example, parents should be able to determine which categories of content they wish to be filtered in their own home. In addition, filtering for a 5 year old should not be the same as filtering for a 14 year old, all of this needs to be taken into consideration by the Industry when developing products that are user friendly for those who are not computer savvy, like most parents.

Regarding the controversy that might arise relating to whether children's rights of access to information and free expression are illegitimately restricted by school or library policies that use filtering, age verification or white lists to limit access to potentially "harmful" materials online, we believe and follow

the principle set forth with UN Convention promoting that we should deal with children rights issues "in a manner consistent with the evolving capacities of the child". Therefore, we recognize children's rights to information and free expression, however, the unrestrained use of the Internet might put them in contact with material that might hinder their development and that might not be consistent with their maturity levels at a certain time.

Privacy

We favor the promotion of legislation and/or self regulation initiatives that would give parents more control over what information is collected from their children online and how such information may be used. Operators of websites and social networks that collect personal information from children should follow a certain number of principles, which should include: a clear and available privacy policy, parental consent to collect information from a child, possibility of deleting a child's personal information, keeping confidentiality and integrity of information collected from children, etc.

Nevertheless, we believe that when we talk about children's use of interactive technologies and privacy a great deal still needs to be done in order to raise awareness amongst children and young people about the need to protect their personal information online. From our experience with kids in schools they see no harm in revealing very personal information for all to see in their favorite social network profiles, for example. We believe that changing this way of thinking is part of what we have to do with our campaigns directed at promoting digital citizenship amongst children and young Internet users.

Electronic Frontier Foundation Position Paper
Oxford Internet Institute workshop on "Child Protection, Free Speech and the Internet"
Lee Tien, Senior Staff Attorney (tien@eff.org)
Sept. 20, 2009

• What is the nature of your interest or experience in this field?
I am a senior staff attorney for the Electronic Frontier Foundation (EFF), a U.S.-based online civil liberties group. I specialize in civil liberties issues such as freedom of expression and privacy. EFF generally has been very active in protecting free expression on the Internet, including the right to express oneself and to receive information anonymously, and in criticizing "censorware" (i.e., filtering products). As an EFF attorney, I have participated in numerous free expression cases, including legal challenges to U.S. laws aimed at restricting online sexual expression. I have also worked on cases seeking to protect individuals' rights to privacy, including privacy of communications and of communications records. I have also written legal articles about mature minors' rights to receive information and the right to express oneself anonymously.

• Are there particular values or principles (ethical, legal or constitutional) that underlie your work?
EFF's work in this area is oriented mainly by the principle that individuals' rights to communicate and to receive communications from others must be protected against interference by public authority, and be permitted regardless of frontiers. We do not, however, agree with every aspect of U.S. First Amendment law. For example, we disagree with the U.S. Supreme Court's conclusion in *United States v. American Library Association* (2003) that the Children's Internet Protection Act (CIPA), which required libraries and schools receiving certain kinds of government funding to install technical protection measures to protect children against harmful-to-minors content online, is consistent with the U.S. First Amendment. We also believe that CIPA is inconsistent with international standards of freedom of expression.

• What are the issues/policies or laws that you see as most problematic in terms of creating or illustrating a conflict between online child protection and free speech?
We see three main problematic areas.
1) As a political matter, child protection generally is viewed as such a worthy and important goal that legislation tends to be overbroad and thus unduly restrictive of both minors' and adults' rights of free expression. Elected officials have strong incentives to support child protection legislation, but diffuse incentives to ensure that the legislation comports with human rights; if such laws are challenged or overturned via judicial review, politicians can and will blame the courts and repeatedly pander to the public with new legislative initiatives. We saw this pattern with U.S. federal laws like the Communications Decency Act (CDA) and its successor, the Child Online Protection Act (COPA), numerous U.S. state and local laws aimed at "violent videogames," and the repeated attempts in Australia at to introduce and then widen a universal Web blocking infrastructure for material "unsuitable for minors." The threat to civil liberties is

not unlike that seen when governments invoke the need to protect against terrorists, which in the United States led to the USA-PATRIOT Act.
2) As a structural or institutional matter, we are concerned that intermediaries like ISPs, online social networks, and financial service providers are so vulnerable to political and social pressure regarding child protection that they will restrict expression or invade their users' privacy in order to avoid government regulation or informal sanctions such as negative publicity. In this way, government may induce or coerce an intermediary or class of intermediaries to restrict users' rights—yet the direct source of the restriction on users would be the intermediary itself (often not a government actor). In the United States, such indirect, extra-legal regulation can hinder legal challenges because constitutional rights are defined largely as rights against government action. Moreover, such government action may not take the form of publicly promulgated laws or regulations promulgated: they might be private threats of enforcement or shaming that lead to private deals less transparent than public laws or regulations. We are generally concerned that these kinds of private bargains between governments and intermediaries will reflect the parties' own interests while neglecting the interests and rights of users excluded from the process.
3) EFF is particularly concerned about the availability of technologies and tools for private and privacy-protecting communication and association, which are crucial to political, religious and cultural dissent around the world. In particular, the ability to protect a speaker's real-world identity from disclosure is an inviolable part of freedom of expression: anonymity not only protects against retribution but fosters respect for private life and protects personal data. Having the legally protected right to private anonymous communication or association, however, is not the same as having the practical ability to communicate or associate privately and anonymously. This issue is not limited to the child protection arena: other policy drivers, such as cyber-security and spam reduction, also target private and anonymous communication. China and Iran's efforts to track down dissenters are obvious examples as well.

• Might any of these conflicts be avoidable, e.g. through the use of improved legislative instruments or greater clarity and accountability in processes of self-regulation?
Yes, but we are not optimistic given the political and socio-technical conditions mentioned above.

• What are the issues where you think there might be most scope for finding some common ground?
The need to protect the rights to communicate and associate freely, privately and anonymously.
The authority of government to protect the vulnerable, subject to due process and the rule of law.
The principle of proportionality or precision: As discussed more fully below, the regulation of categories of expression thought to be "unprotected" entails several distinct steps. That the category may be prohibited under the law is only the first step; it is always a distinct question whether or not a particular work of expression sought to be prohibited actually falls within that category. Moreover, when a regulation or regulatory scheme is aimed at such proscribable expression, such as obscenity or child pornography, it is also always a distinct question whether that regulation or scheme is sufficiently narrowly targeted, or instead sweeps so broadly that it includes other, entirely lawful expression.

• At the international level, are there certain key principles which we ought to be defending above all others?
One key principle is the right to communicate freely, privately and anonymously. Another key principle is that government action must be subject to due process and the rule of law. U.S. law protecting free expression explicitly combines these principles in what might be called "First Amendment due process," which seeks to guard against imprecise and overbroad government interference with expression. For example, obscenity as a category can be proscribed under U.S. law. But that does not mean that any law that seeks to protect the public against obscenity is valid. The law must still be very narrowly tailored to obscenity, a type of proportionality requirement. Moreover, whether any particular picture is legally obscene is another question, and the would-be censor has the burden to show that a given work is legally obscene. U.S. law takes the perspective that because the censor's job is to censor expression, he or she is unlikely to be as sensitive to freedom of expression as a neutral judge.

• In relation to child pornography, are blacklists and notice and take down services or other quasi judicial or voluntary schemes legitimate tools in the eradication of child abuse, and if so, what should be the proper scope and legal status of these measures?
The legitimacy of any tool aimed at speech depends on its design, its use, and its accountability. It also matters whether such tools are truly voluntarily used. Government should not, for instance, subject speech to prior restraints without meaningful independent judicial review. Even if such tools are truly used voluntarily by intermediaries, there is a significant risk that lawful communications will be affected. To mitigate that risk, there must be meaningful accountability in the use of such tools. In general, EFF opposes schemes under which intermediaries are granted immunity from liability, disclosure and investigation if they use speech-restrictive tools.

• Attitudes towards and legal treatment of pseudo-images of child pornography and non photographic visual depictions of child pornography.
EFF opposes laws restricting such visual depictions as child pornography, following the reasoning of the U.S. Supreme Court's decision in *Free Speech Coalition v. Ashcroft* (2002). Child pornography has a special legal status in the United States because it is intrinsically related to the sexual abuse of actual children, not because of its semantic or representational content or meaning. Thus, EFF views such laws as attempts to define a class of expression as harmful in itself, rather than as expression intrinsically related to the sexual abuse of children. A contingent and indirect link to possible future crime is not sufficient to limit fundamental human rights.

• The role of filtering products and the extent to which they should ever be preinstalled, preconfigured and set by default at network level by service providers or on end user machines, or even both.
EFF is generally hostile to filtering products, i.e. "censorware." Although we recognize that their purely private, uncoerced use is legally permitted in the United States and elsewhere, such private censorship nevertheless harms expression and harms those who are censored. No computer program can or should decide whether expression is lawful or unlawful. Censorware is inherently imprecise and is virtually guaranteed to censor wholly lawful expression even if intended to censor only unlawful expression, again raising proportionality concerns. In the real

world, censorware may also reflect the subjective judgments of the companies or human beings who supply the data for its filters, which usually intentionally includes lawful but disfavored expression. Furthermore, censorware inexorably seeks to deny access to tools for private or anonymous communication, because such tools usually also allow users to circumvent censorware. More generally, censorware systems usually cannot permit users to have access to general-purpose computers outside of the censorware regime because then these computers could be used as proxies to escape the control of the censorware. The result is not only a default environment of less open computers, but also of public discourse that is distorted by the omission of whole classes of information and where speakers inevitably self-censor in order to protect themselves from the damage caused by triggering default filters. EFF expressed some of these views recently in comments on the Child Safe Viewing Act.
http://www.eff.org/deeplinks/2009/06/eff-comments-child-s

In addition, the technical infrastructure required to impose network level controls (or widespread or compulsory end user filtering, such as China's proposed Green Dam Youth Escort software) lends itself to co-option in wider censorship practices, either due to political pressure within the country of origin, or through technical export to countries with poor traditions of upholding human rights.

• Whether children's rights of access to information and free expression are illegitimately restricted by school or library policies that use filtering, age verification or white lists to limit access to potentially 'harmful' materials online.
Some restriction of children's access to online materials is appropriate in schools and libraries, but such restrictions must be carefully crafted. What is inappropriate for a 6-year-old may be fully appropriate for a 13-year-old. We have argued that adolescents generally have the right to access information about reproductive health, sexual behavior, religious issues and similar subjects precisely because such information is critical to their becoming adults.
http://w2.eff.org/Censorship/Censorware/20010306_eff_nrc_paper2.html
Under U.S. First Amendment law, and as a general principle in, for example, Article 26 (3) of the Universal Declaration of Human Rights, parents have a superior role to the government in making decisions about their children's intellectual development. As explained above, EFF believes that censorware and white lists are too imprecise or too overbroad to effectively address constitutional concern in public institutions, and have unintended consequences on, for example, a child's "freedom to seek, receive and impart information of all kinds." U.N. Convention on the Rights of the Child, Article 13.

• The criminal use of encryption technology and related privacy issues.
Encryption and other technologies of private or anonymous communication and association should be generally available to the public. Measures intended to deter criminal use of such technologies must be narrowly targeted to address demonstrated problems and must not create practical, real-world disincentives for the creation or adoption of privacy-protective technologies and practices in general. One of EFF's most important cases, which challenged U.S. government encryption export controls, illustrates the danger. Although export controls targeted foreign encryption users and did not purport to regulate domestic encryption use, U.S. entities as a

practical matter did not want to bear the added costs of producing equipment that they could not export. As a result, domestic users had significantly less access to strong encryption.

• The place of children's rights online in the wider range of digital rights online, and in particular how these are to be balanced against other international instruments and treaties.
EFF believes that human rights apply to all age groups, and that, as a vulnerable group in society, children need a strong defense of their rights to privacy, to free expression, and to participate in culture, such as via online social networks.

CHILD PROTECTION, FREE SPEECH AND THE INTERNET
Oxford Internet Institute
October 2, 2009

National Center for Missing & Exploited Children
699 Prince Street
Alexandria, Virginia, 22314
U.S. A.

What is the nature of your interest or experience in this field?

The National Center for Missing & Exploited Children (NCMEC), by authority of the U.S. Congress, serves as the U.S. clearinghouse on issues relating to missing and exploited children. Specifically, Congress authorizes NCMEC to operate the CyberTipline, which receives reports from both the public and Electronic Service Providers (ESPs) on crimes against children on the Internet. Most of these reports are related to child pornography. ESPs based in the U.S. are required by federal law to send specific information regarding apparent child pornography on their networks to NCMEC's CyberTipline. Almost 600 ESPs are registered with the CyberTipline. Registration allows them to make reports via an encrypted reporting form, a security measure that enables ESPs to include the suspected contraband in their reports. NCMEC analysts review the CyberTipline reports, conduct open-source and public database searches to add value, and forward each report to the relevant federal, state or local law enforcement agency which has jurisdiction to investigate the potential crime. NCMEC also forwards CyberTipline reports to law enforcement in other countries. To date NCMEC has received more than 731,000 such reports; approximately 90% of these relate to child pornography. NCMEC applies the definition of child pornography under U.S. federal criminal law.

NCMEC is also authorized by the U.S. Congress to operate the Child Victim Identification Program (CVIP), which assists law enforcement and prosecutors in securing convictions for child pornography offenses by providing information about identified child victims depicted in images seized by law enforcement. CVIP maintains information relating to the cases in which approximately 2,500 child victims were identified by law enforcement. NCMEC/CVIP does not collect or store victim information. Rather, NCMEC/CVIP assists law enforcement and prosecutors by providing the name of the law enforcement officer who identified the child.

In addition, the U.S. Congress authorizes NCMEC to share Uniform Resource Locators (URLs) of webpages containing apparent child pornography with ESPs for the purpose of preventing their further distribution on the Internet. ESPs are not required to participate in this voluntary program. If they choose to participate, ESPs are authorized by the U.S. Congress to use these URLs to stop the transmission of apparent child pornography images. To date, 65 ESPs are participating in NCMEC's URL-sharing program, as well as law enforcement agencies in Canada, Australia, the United Kingdom, Norway and Denmark. CIRCAMP (Cospol Internet Related Child Abusive Material Project) also utilizes NCMEC's URL list. For more details on NCMEC's URL-sharing program, please see the attached Exhibit.

NCMEC is an active collaborator with law enforcement and non-governmental agencies in other countries on issues concerning the sexual exploitation of children through its membership in the International Association of Internet Hotlines (INHOPE). NCMEC has been a member of INHOPE since its creation in 1999 and is a proponent of more efficient information-sharing and uniform best practice guidelines.

Are there particular values or principles (ethical, legal or constitutional) which underlie your work?

NCMEC operates on the principle that children have the right to be free from sexual victimization. This is supported by the U.S. Constitution, laws and judicial decisions which demonstrate the value of children as individuals and the obligation to protect them as vulnerable members of our society. NCMEC complies with U.S. federal and state laws. It was created under these laws to be a public-private partnership and authorized by the U.S. Congress to perform specific functions in furtherance of the goal of protecting children.

NCMEC is neither a governmental agency nor a law enforcement agency. It does not investigate or prosecute crimes against children. It assists law enforcement in their responsibilities and educates the public about these issues.

In the U.S., the sexual exploitation of children and the production, possession and distribution of child pornography is a crime. The size and scope of the Internet make the investigation and prosecution of these crimes very difficult, particularly when law enforcement is working with limited resources. NCMEC believes that the best approach to these crimes is a comprehensive strategy that combines law enforcement efforts to investigate and prosecute offenders with voluntary industry initiatives to target the distribution of these images.

What are the issues/policies or laws which you see as most problematic in terms of creating or illustrating a conflict between online child protection and free speech?

The phrase “online child protection” encompasses a broad range of ways that children are victimized on the Internet --- including enticement, bullying, exposure to harmful content, etc. Child pornography is also a way that children are victimized and is a more narrow issue. The U.S. Supreme Court held that child pornography is not protected speech. However, many in the U.S. remain unaware of the size of the problem of Internet child pornography and the nature of these images, falsely assuming that most of these images depict adult women portraying themselves to look like young teenage girls.

There is also a general misconception that those who “merely view” sexually abusive images of children are not culpable because they did not produce the images. This perception fails to acknowledge the fact that some children are victimized solely to satisfy the demand from the offenders who “merely view” the images. People who have a sexual interest in children often use the Internet to connect with like-minded individuals, share images and videos, and collaborate on the best ways to gain access to children and maintain their silence. The images are shared as trophies of their victims and may inspire others to victimize children.

Might any of these conflicts be avoidable, e.g. through the use of improved legislative instruments or greater clarity and accountability in processes of self-regulation?

NCMEC is always vigilant of the need to stay within the strict U.S. Constitutional constraints against infringement of speech that is protected by the First Amendment. NCMEC is particularly cautious in the operation of its URL-sharing program. For example, U.S. federal criminal law defines child pornography victims as under the age of 18. However, NCMEC's URL list contains webpages with images of only pre-pubescent children. This eliminates any concern that webpages depicting adults (age 18 or older), which may be protected speech in the U.S., are affected. Also, under U.S. federal criminal law the definition of child pornography images includes a broad range of sexually explicit conduct. However, a more narrow range of conduct is required to meet NCMEC's criteria for inclusion its URL list. See attached Exhibit.

Conflict can be avoided through a greater widespread understanding of how children are victimized by the continuing distribution of images depicting their sexual abuse or exploitation. This can be achieved through meaningful public dialogue between the Internet industry, child protection groups, civil liberties advocates and the criminal justice system.

What are the issues where you think there might be most scope for finding some common ground?

NCMEC believes that there can be common ground in the interest of child victims worldwide. These children deserve every possible effort to eliminate the evidence of their abuse that others use for their own sexual gratification.

At the international level, are there certain key principles which we ought to be defending above all others?

The key principle is that the sexual exploitation of children is a crime, that sexually abusive images are the memorialization of this crime, and that both should be criminalized and prosecuted vigorously. A related principle is that the possession and distribution of sexually abusive images is not a victimless crime – each child depicted is revictimized each time the images are traded, downloaded and viewed.

The impact of this ongoing victimization is best demonstrated by the child victims (and their parents) who choose to speak out about it. Additional trauma is inflicted on these children (into adulthood) as images of their sexual abuse are continually traded online and collected by countless individuals who have a sexual interest in children and wish to witness his/her victimization. The circulation of these images, and the resulting trauma to the victims, will continue for the foreseeable future. Victims' first-hand accounts of the pain inflicted are critical to removing the phrase "they're just pictures" from the public dialogue.

CHILD PROTECTION, FREE SPEECH AND THE INTERNET
Oxford Internet Institute
October 2, 2009

National Center for Missing & Exploited Children
699 Prince Street
Alexandria, Virginia, 22314
U.S. A.

EXHIBIT

NCMEC's URL-Sharing Program

Pursuant to its authorization by the U.S. Congress, NCMEC provides a daily list of active webpages containing apparent child pornography to the Electronic Service Providers (ESPs) participating in the URL-sharing program. Each ESP agrees to utilize this list to help reduce the proliferation of sexually abusive images of children online.

The webpage must meet certain criteria in order for NCMEC to place it on the list. First, the page must contain images, whether photographs or videos, of pre-pubescent children (i.e., a child who is not yet showing indicators of sexual maturation). Once this threshold is met, in order for the URL to be placed on NCMEC's list the images must depict one of the following (drawn from the U.S. federal law defining child pornography):

1. Oral, vaginal, or anal penetration and/or sexual contact involving a child, including contact with the genitals, mouth, or digits of a perpetrator, and/or contact with a foreign object.

2. An animal involved in some form of sexual behavior with a child.

3. Lewd or lascivious exhibition of the genitalia or anus of the child.

The process is as follows:

When a member of the public or an ESP reports a webpage containing apparent child pornography to the CyberTipline, a NCMEC analyst visits the webpage to verify that it contains apparent child pornography. If it does, the analyst conducts public records database searches to add value, finalizes the CyberTipline report, and makes the report available to law enforcement for investigation.

If after seven days there has been no indication that law enforcement intends to investigate the webpage, the webpage is automatically revisited to determine if the content has changed. If the webpage remains unchanged, meaning that images of apparent child pornography still exists at that URL, then the URL is placed on the daily list. If the webpage is different than what was documented seven days earlier, a NCMEC analyst accesses the webpage and conducts a visual review based on the above criteria. If these criteria are not met, the URL is not placed on the list.

A new, current list is generated every 24 hours and is therefore dynamic. Each day, NCMEC verifies the content of each webpage on the URL list. If any changes to the

images are detected, the URL is automatically removed and subjected to a retest. Each business day a NCMEC analyst reviews any URLs that were removed by the system to confirm that the criteria stated above is met. If the criteria is met after this visual review, the URL is placed back onto the URL list.

NCMEC provides participating ESPs with a way to access the daily list over a secure mechanism. NCMEC cautions ESPs to use only the current daily list, because the list will change.