Children and the Internet

The Internet is an increasing part of today's culture, especially for children and youth, for whom schoolwork, online gaming, and social networking are among the most popular activities. However, the lack of common agreement about the right approach to educating and protecting children adds further challenges to a child's online experience and expression. Additionally, cultural and geographical differences in legal and social norms reflect the fact that there is no universally accepted view of what defines a person as a child, or of what is appropriate for children, making "inappropriate content and behaviour" hard to define.

While some online crimes are cross-border in nature and so require global attention, at a national level, policy approaches to regulating content have so far predominantly employed a range of filtering techniques to limit access to or block Internet content. In addition, while local institutional or individual parental computer level filtering is often advised (and should, principally, be used in preference to network level filtering), neither these efforts nor national and local level filtering methods are 100% effective at regulating undesirable content, as at times they tend to under- or over-block content. Filtering at the network level has additional adverse effects. It is therefore vital for parents, educators, guardians, peers and the state to educate children and young people on risks and responsibilities they may encounter when using the Internet. This approach could empower the youth to recognize and avoid dangers, while equipping them with online literacy skills to responsibly reap the benefits Internet activity offers.

Introduction

The Internet, for children and adults alike, is a hugely important medium. Children and young people now frequently use the Internet to:

- Learn (by having access to information, knowledge, opinions, education tools, and even teachers);
- Communicate (express ideas, share information and experiences);
- Interact socially with friends and peers;
- Innovate, create and share content;
- Play and be entertained (games, movies, music, books, etc.);

Increasingly, these activities are occurring outside the home or school, beyond the traditional desktop computer, on handheld devices such as smart phones and tablets.

Compared to other technologies that supply content, such as radio and television, the Internet presents parents, guardians and educators unique opportunities to take a more direct role in deciding what their children can see and do. For example, they can direct the child toward beneficial and entertaining content suitable to each child's age, culture, intellectual capacity, education, etc. It also provides opportunities to educate children about the constructive use of the Internet and to provide guidance on how to avoid risky online behaviour and inappropriate content.

It is of key importance that everyone – parents and guardians, teachers, institutions and governments – work together to create safe and accessible environments for children and young people wherever they are; at home, at school, or in public facilities such as libraries or Internet cafés. It is everyone's responsibility to create these environments, so that all children and young people can enjoy, and harness the positive aspects of the Internet.

Further, while it is important to be alert to the potential risks involved in children going online, it is also important to keep things in perspective. Education, common sense and clear guidelines are the best place to start. While much work has been done on how best to protect children, the Internet Society believes more can be done to empower children and young people in order to protect them from potentially harmful material on the Internet and, at the same time, allow them to make full use of the Internet's capabilities and values.

What is considered a 'Child'?

One of the most challenging issues is determining what a child is as approaches vary significantly depending on societal and disciplinary definitions.

The United Nations Convention on the Rights of the Child (CRC) states in Article 1: "a child means every human being below the age of eighteen years unless under the law applicable to the child, the majority is attained earlier". Notwithstanding the benign purposes of that definition, setting the age limit to 18 years old could be debatable from many perspectives.

Naturally, there are other definitions of a child, however each of them defines the term from a different scientific perspective. Psychology, for instance, adopts certain criteria relating to psychological maturity and development, whilst biology shows preference to physical development. From a non-scientific point of view, moralists support notions of conscience and freedom of consent in determining what a child is.

Children's use of the Internet

It appears that getting agreement on what defines a person as a child is one of the largest obstacles to achieving effective child protection. But however we define the term, we certainly know that children and young people routinely use the Internet, as it has become an essential part of modern life. Children's ability to access the Internet has grown rapidly, and most young people frequently access the Internet.

Children get involved in a wide variety of activities on the Internet, and many overlap each other, as Web 2.0 platforms increasingly are becoming a part of today's youth culture. A 25 country survey conducted by *European Union Kids Online* and funded by the European Commission's Safer Internet Programme suggests that top activities for children and youth using the Internet are: schoolwork (92%), playing games (83%), watching video clips (75%) and social networking (71%). 59% of European children who use the Internet have their own social network profile. Only 28% of 9-10 year olds, but 59% of 11-12 year olds, have a social network profile, suggesting that it is the start of secondary school rather than the minimum age set by popular providers, that is a major trigger for social networking.[1] To this end, identifying and establishing norms that can inform online interactions should become an integral part of a child's education and must begin in the primary grades.

[1] More statstics can be found on http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20Online%20reports.aspx

An important role in enabling children's safety on the Internet is to help them to understand the concepts of risk and safety online, which will allow children make independent informed decisions. Internet safety education is critical in protecting young people against online threats; both external threats, such as 'inappropriate' content and activities (e.g. gambling) or contact with the 'wrong' people (e.g. bullying, stalking, scams), and internal threats, such as disclosure of too much personal information. By working together with children, and listening to their needs and learning from their experience, we can shape an environment for children, enabling them to make the most of the opportunities that the Internet offers, while behaving in a safe and responsible way. At the same time, such an environment can help those children who take advantage of the Internet to commit 'bad acts' to understand the true impact of their actions on more vulnerable subjects.

Finally, it is important to bear in mind that the Internet is not an 'evil' tool, exposing children to unprecedented dangers. This idea is in line with the resilience-based school of thought , which illustrates how "preserving adaptive capacity – the ability to adapt to changed circumstances while fulfilling once core purpose – [is] an essential skill in an age of unforeseeable disruption and volatility".[2] Based on this theory, when it comes to child safety online, legislating and regulating might, at the end, be counterproductive. It is impossible (and potentially futile) to seek to ban every single activity that potentially exposes children to dangers in the Internet; a much healthier, resilient-based approach sees education and empowerment as the tools that will enable parents, educators or the state to address such issues relating to the safety of children in the Internet. We should strive towards engaging children with the Internet at a gradual pace and use resiliency strategies to teach them how to cope with the online environment and its dangers. To this end, teaching children about the importance of 'netiquettes' and instilling to them the notion of "think before you click" should be our primary goal.

With this in mind, the sections that follow illustrate some of the dangers that children face online.

Issues surrounding the definition of child abuse and pornography

The first international attempt to define 'child pornography' as a form of child abuse was that of the Optional Protocol (OP) to the Convention on the Rights of the Child (CRC)[3] on the sale of children, child prostitution and child pornography. However, a more recent definition under the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse[4] was opened for signing in October 2007, provides greater clarity. Article 20 defines child pornography as, "any material that visually depicts a child engaged in real or simulated sexually explicit conduct or any depiction of a child's sexual organs for primarily sexual purposes".

As the conduct is generally covert and there is also a lack of a uniform definition of what is to be classified as child sexual abuse material, it is unclear how widespread such material is. This difficulty is compounded by the lack of data from many parts of the world regarding the production and distribution of child sexual abuse material; and a shifting global pattern of production and consumption of such material. The rapid development of digital camera and computer technology, which has provided expanded access and allowed for the creation of digitally generated or modified images makes it even harder to gather reliable statistical information about the scale of the problem.

Additionally, the lack of uniform national legislation or global controls explicitly outlawing child sexual abuse material makes child protection online a very difficult task. Only some nations or

[2] Andrew Zolli & Ann Marie Healy (2012). " *Resilience: Why Thins Bounce Back*", Free Press,

[3] http://www.unicef.org/crc/index_protocols.html

[4] http://conventions.coe.int/Treaty/EN/treaties/Html/201.htm

regions have introduced legislation criminalizing child sexual abuse material. While some countries have started the process of legal reform, most countries still rely on out-dated legislation against obscenity, which is not adequate to deal with sexual offences or abuse committed via the Internet.

The simple lack of a clear agreement at the governmental level about the dimensions of the problem and the appropriate legal response only serves to emphasize the importance of providing parental and educational guidance to children. It is important to ensure they will know how to respond if they encounter child sexual abuse material while using the Internet, or if they encounter perpetrators who might try to lure them into dangerous situations.

Other potential threats

Children and young people face a broad spectrum of risks when they use a computer. Some are threats to their safety or privacy. Still others may result from children intentionally or unintentionally violating laws such as copyright or defamation. These can also have serious consequences.[5]

What are the risks to children and young people?

- Exposure to inappropriate images or content, whether inadvertently or deliberately.
- Solicitation by sexual predators in chat rooms, other forms of social media, and by email.
- Online bullying or harassment.
- Inappropriate disclosure of personal information and data theft (through over-sharing or other means).
- Spyware, viruses and malicious software.
- Scams
- Excessive commercialism: advertising and product-related websites.
- The consequences of the temptation to engage in piracy of software, music or video.[4]

Youth is the fastest growing age group using the Internet; yet where they lack awareness and have limited ability to assess risk and make decisions, they are vulnerable. Multi-stakeholder co-operation at the local, national and international level is an effective way to create awareness of the importance of child protection issues in some regions of the world, Furthermore, policing offences requires multi-agency co-operation at the local and national level, while on an international level, cooperation and information-sharing is vital in dealing with child protection.

No one size fits all approach to dealing with child protection

There are cultural and geographical differences, both in relation to constructs of childhood and the perception of what are appropriate or acceptable practices. When it comes to content, and more specifically “inappropriate content”, a population of children is not homogenous. Each child is different – different ages, education, language, culture, religion, maturity, experiences, interests, etc. – and individual children change rapidly as they mature and develop. The determination of what content is appropriate for an individual child is best left as the responsibility of the parents, guardians and educators who know the child.

The proliferation of new technologies, the inevitable lag in developing policies surrounding them, plus the diversity of cultures and levels of development highlights the complexity of finding

[5] Threats of this type are significant, but beyond the scope of the present paper.

solutions. On the positive side, it is equally important to develop and publicise culturally, linguistically, age relevant content to make it attractive and readily accessible.

Approaches to controlling access to undesirable content

Many countries around the world have chosen to develop national approaches to Internet regulation, with varying degrees of success and sometimes with unintended consequences. This can be observed in the rapidly rising number of countries that have chosen the approach of simply limiting access to Internet content in recent years. Additionally, an increasing number of countries have tried to impose Internet filtering, a technical approach to controlling access to content. Generally, three techniques are commonly used to block access to websites: IP blocking, DNS filtering, and URL blocking using a proxy. Keyword blocking, which blocks access to websites based on the words found in requested URLs, or blocks searches based on a list of blacklisted terms, is a more advanced technique that a growing number of countries are employing. These methods can be implemented at different locations; for example, at the ISP, by an institution or at the specific Internet-connected device.

Many different filtering techniques exist, all aiming to restrict access to certain websites. Some are based on a "bad site" list that ISP's or authorities create and deploy at the network level, but parents, guardians, educators, or other authorities also have access to programs and tools able to monitor, track and block access to specific online activities on devices used by children; for example:

- Proxies and software that can allow or block specific sites and protocols (including anti-virus protection, email spam filters, pop-up blockers, anti-spyware, cookie deletion software, etc.)
- Content filtering software that finds and blocks specific content or websites
- Configuration options to set site privacy and monitoring features (e.g., Google SafeSearch filter, Privolock)

However, filtering can never be 100% effective. Filtering technologies are prone to two simple inherent flaws: under-blocking and over-blocking, Under-blocking refers to the failure of filtering to block access to all the targeted content. On the other hand, filtering technologies often block content they do not intend to block, which is known as over-blocking. Both these failings occur because many blacklists are generated through a combination of manually designated websites and automated searches, and therefore often contain websites that have been incorrectly classified. Additional issues arise where other content is hosted from the same IP address or domain. Furthermore, filtering methods do not remove the illegal content from the Internet,[6] and are prone to circumvention. They also have the potential to restrict free and open communications inadvertently or deliberately, and thereby to limit the rights of individuals or minority groups.

Because network filters are often proprietary and/or use secret “black lists”, there is often no transparency in terms of the labelling and restricting of sites. This lack of transparency is particularly troubling when the corporations that produce content filtering technology work alongside undemocratic regimes in order to set-up nationwide content filtering schemes. Most states that implement content filtering and blocking augment commercially generated block lists with customized lists that focus on topics and organizations that are nation or language specific.

While Internet use at school is usually filtered or supervised, many children access the Internet from several different locations and on different devices where there may be no filters and little

[6] A different domain name pointing to the same Internet address could be established within minutes.

supervision. Children and young people are increasingly accessing the Internet via other Internet enabled devices; e.g., smart phones, tablets and gaming devices. This means that, even if filtering is deployed on the home or school computer, children and young people likely will still be able to access the unfiltered Internet through other means or perhaps even by circumventing the filters deployed on the computer. It is, therefore, important to help educate children about how to behave online and to engage them in discussing the problems they may encounter.

It can be argued that filtering at the network level, such as DNS filtering, also causes network instability, encourages fragmentation, and erodes the foundation of the Internet.[7] Other approaches to controlling content such as domain name seizure, intended not only to protect young people, suffer from most of the same problems as DNS filtering, including easy circumvention, failure to solve the underlying problem, and encouragement of a shadow network out of reach of law enforcement.

While software may be able to block specific high profile websites, there is no solution yet available that is robust over time or completely effective. Technologies are not able to accurately identify and target specific categories of content found on the billions of websites and other Internet applications such as news groups, email lists, chat rooms, instant messaging and social media. Filtering is never a substitute for good parental involvement and advice. In any case, these methods do not remove the objectionable or illegal content from the Internet; they only make it harder to access.

Finally, the Internet Society is concerned that child online protection can be a gateway or a back door to further government controls online. This said, children and young people cannot be made 100% safe online by blocking of content. However, we can improve the safety of children and young people online by empowering children, parents, guardians educators and peers to identify and deal with harmful content on computers, the Internet and mobile phones, and how to use technology both safely and responsibly, and by making available easy to use adjustable tools to manage access and content.

Recent policy guidance

In 2011, the OECD released a report entitled *The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them*[8], and in 2012, the OECD adopted a *Council Recommendation on the Protection of Children Online*[9] establishing three key principles:

- empowerment
- proportionality and fundamental values
- flexibility.

Further, the Recommendation[10] calls on governments to:

- demonstrate leadership and commitment through their policies;
- support a co-ordinated response by all stakeholders; foster consistency and coherence of domestic child online protection initiatives across public and private stakeholders;

[7] More Information can be found on DNS blocking on http://www.internetsociety.org/what-we-do/issues/dns/finding-solutions-illegal-line-activities

[8] http://www.oecd-ilibrary.org/science-and-technology/the-protection-of-children-online_5kgcjf71pl28-en

[9] http://webnet.oecd.org/oecdacts/Instruments/ShowInstrumentView.aspx?InstrumentID=272&InstrumentPID=277&Lang=en&Book=False

[10] http://webnet.oecd.org/oecdacts/Instruments/ShowInstrumentView.aspx?InstrumentID=272&InstrumentPID=277&Lang=en&Book=False

- foster awareness-raising and education as essential tools for empowering parents and children;
- support evidence-based policies for the protection of children online;
- encourage the development and adoption of technologies for the protection of children online that respect the rights of children and the freedom of other Internet users;
- strengthen international networks of national organisations dedicated to the protection of children online;
- share information about national policy approaches to protect children online and in particular develop the empirical foundations for quantitative and qualitative international comparative policy analysis;
- support regional and international capacity building efforts to improve policy and operational measures to protect children on the Internet;
- better co-ordinate work by the various international and regional organisations and bodies which play a role to support government efforts in this area, and involve non-governmental stakeholders where appropriate.

Empowering children: a constructive role for parents, guardians and educators

Perhaps the most effective way to deal with perceived problems arising from Internet use is to empower children and young people so they know how to safeguard themselves and their friends. Empowerment techniques include teaching them about legal boundaries in age appropriate language, as well as discussing openly their communities' cultural, moral and ethical norms and expectations. It is the role of parents, educators, the private sector, governments and others to help young people learn to recognise and respect these boundaries and norms. Empowering children and young people also helps prevent them from being victims of other threats including scams, spyware and malware.

While effective strategies are emerging that parents can use to manage their children's use of the Internet, so too are children's tactics for evading, or resisting this family oversight. 'This is further complicated by the fact that children often have more confidence and expertise in using new media than do their parents. Yet children and youth usually will have trust relationships with adults and peers whose advice and opinions they value (trusted influencers). It is important that these trusted influencers are themselves aware of potential risks and solutions, and educated about how to effectively convey the information to those who look to them as role models and sources of reliable information and advice. It is also important to recognise that these trusted influencers will change over time. As a child approaches the "teen years", their peers will likely become the stronger influencers.

In addition, parents, guardians, educators and trusted influencers should take an active role in teaching children and young people about the risks they may face from sexually explicit materials online and from Internet predators and scammers and how to avoid them. Equally important, children should also be educated about how to communicate privately with known friends, and to be careful about sharing personal information on the Internet. Of course, to teach effectively it is important for parents, guardians, educators and peers to be computer literate.

At least two factors challenge parents' ability to control their children's Internet access and use. The first is that while parents are responsible for their children's safety, they must also respect their children's growing independence and rights to privacy.

The second is the fact that few parents fully understand their children's Internet culture.[11] Children's and young people's use of social networks is often baffling to parents. In addition, there are huge generational gaps in attitudes toward privacy, confidentiality and an individual's rights over the data they own and share. The issues of safety, privacy, online predation and cyber-bullying are complex, both technically and psychologically, and parents may find it a struggle to keep up. These factors point to an urgent need to encourage parents to engage with their children and to discuss their online activities, whatever their level of experience. Getting involved will allow parents, guardians, educators and other trusted influencers to keep children and young people out of harms way.

It is equally important to empower children by equipping them with online literacy skills. This includes teaching and encouraging them to master available ICT tools, and how to make good decisions (alone and in groups), so that they will grow to become the next generation of responsible and trusted influencers.

Conclusion

While working directly with children in their families, in schools and in other settings that permit one-on-one interaction and counselling, there are a range of actions that governments, not-for-profits and community organizations could take to create awareness and build capacity to help children and young people to benefit from the Internet in a safe environment. The following are examples of some initiatives that might be considered:

- Involve all stakeholders in community awareness building activities: government agencies, the private Internet sector, NGOs, community groups and the general public.[12]
- Establish Internet hotlines to support the public in reporting offences on the Internet, as well as for counselling and advice.
- Encourage educational programs involving ISPs and law enforcement to develop best practices in dealing with illegal content and conduct.
- Setting up of Internet sites or platforms to provide an educational platform for kids, teenagers, parents and teachers. These sites should have current and regularly updated content on Internet Safety with self-guided videos in various regional languages.

The Internet changes so rapidly that technological measures are unlikely to be able to keep up. More effective and durable measures are those that build on the family, the community, education and empowerment so that children and young people will make good choices and benefit from the generative power of the Internet.

[11] The ways in which their children use the Internet and mobile phone to work, play and socialise

[12] For example of Good practices of Internet Safety awareness website please visit www.kidsap.org and ECPAT International's Safety Online Handbook

Annex

'Cues and Clues' for Parents, Children and Educators

Below are some tips that parents, teachers (and children) should be aware of relating to the use of the Internet.

- The computer should be at a visible place in the house, so adults can monitor the purpose that is used for.
- Education of what computers are and how the Internet should be used should take place at all levels – children, parents and teachers.
- Parents and teachers should spend time with children in the online environment.
- Parents should (in consultation with their children) set reasonable use and time limits of Internet use.
- Parents and educators should familiarize and educate themselves about the dangers of the Internet.
- Parents and educators should emphasize that the principle 'Don't speak to strangers' also applies in the online environment.
- Parents and educators should forbid their children from downloading and/or uploading pictures without proper supervision.
- Full use of filtering and parental controls should be made both in the house and in the school environment.
- Parents and educators have the obligation to instil to children the need for privacy at a young age, explaining why it is important for children to respect and seek for the right to 'be let alone'.

Internet Society
Galerie Jean-Malbuisson 15
CH-1204 Geneva, Switzerland
Tel: +41 22 807 1444
Fax: +41 22 807 1445
http://www.internetsociety.org

1775 Wiehle Ave. Suite 201
Reston, VA 20190, USA
Tel: +1 703 439 2120
Fax: +1 703 326 9881
Email: info@isoc.org