OECD Digital Economy Papers No. 179

The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them

OECD

https://dx.doi.org/10.1787/5kgcjf71pl28-en

OECD

Unclassified **DSTI/ICCP/REG(2010)5/FINAL**

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development **02-May-2011**

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

DSTI/ICCP/REG(2010)5/FINAL
Unclassified

Working Party on Information Security and Privacy

THE PROTECTION OF CHILDREN ONLINE

Risks faced by children online and policies to protect them

English - Or. English

JT03300896

Document complet disponible sur OLIS dans son format d'origine
Complete document available on OLIS in its original format

FOREWORD

This report follows up on the 2008 Seoul Ministerial Declaration on the Future of the Internet Economy. It will feed related OECD activities such as work by the Working Party on Information Security and Privacy (WPISP) on the evolving privacy landscape and on identity management, by the Committee on Consumer Policy (CCP) in relation to the review of the 1999 Guidelines for Consumer Protection in the Context of Electronic Commerce and by the Committee for Information, Computer and Communications Policy (ICCP) on Internet Intermediaries.

It was prepared by Kristina Irion (Central European University), consultant to the OECD, under the supervision of the OECD Secretariat (Laurent Bernat, Directorate for Science, Technology and Industry). Information related to quantitative data was added by Elodie Prosser.

In addition to OECD member countries, observers, and delegations from the Business and Industry Advisory Committee (BIAC) and Civil Society Internet Society Advisory Council (CSISAC), the Secretariat wishes to thank the group of experts who provided input and advice during the drafting process including Sonia Livingstone (London School of Economics), John Carr (eNasco), Cristina Schulman and Alexander Seger (Council of Europe), Liz Butterfield (Hector's World), Andrea Millwood-Hargrave (International Institute of Communications), Ruben Rodriguez (Inhope), Jules Cohen, Peter Cullen and Julie Inman-Grant (Microsoft), John Palfrey, Urs Gasser, and danah boyd (Berkman Center for Internet and Society), Cristina Bueti and Susan Teltscher (ITU), and Maxime Zabaloueff.

The report was declassified at the 61st session of the Committee for Information, Computer and Communications Policy (ICCP) on 16-17 March 2011.

© OECD 2011

TABLE OF CONTENTS

EXECUTIVE SUMMARY 4
INTRODUCTION 6
PART I. RISKS FACED BY CHILDREN ONLINE 16
Typologies of risks 16
Overview of risks 16
Risks pertaining to children as Internet users 17
Children targeted as consumers on the Internet 25
Information privacy and security risks 26
PART II: POLICY MEASURES TO PROTECT CHILDREN ONLINE 32
The three dimensions of policies to protect children online 32
Multi-layered policies 32
Multi-stakeholder effort 37
Multi-level policies 39
Comparative policy analysis 41
Parallels in countries' high-level policies 41
Definition of a child 42
Combinations of policy measures 42
Use of evidence, policy assessments and performance evaluations 43
PART III: KEY FINDINGS 45
Policy coherence 46
Co-ordination 46
Consistency 46
Coherence 47
Evidence-based policy 47
Quality measurement of risks 48
Policy impact assessments 48
Performance evaluation 48
International co-operation 49
ANNEX I - DESCRIPTIVE OVERVIEW OF POLICIES TO PROTECT CHILDREN ONLINE 51
ANNEX II – TABLES AND FIGURES 76
NOTES 79
BIBLIOGRAPHY 94

EXECUTIVE SUMMARY

An increasing number of children are now using the Internet. They are starting at a younger age, using a variety of devices and spending more time online. The Internet can be a major channel for their education, creativity and self-expression. However, it also carries a spectrum of risks to which children are more vulnerable than adults. Addressing risks faced by children online is becoming a policy priority for an increasing number of governments.

This means facing many complex policy challenges: How to mitigate risks without reducing the opportunities and benefits for children online? How to prevent risks while preserving fundamental values for all Internet users, including the children themselves? How to ensure that policies are proportionate to the problem and do not unsettle the framework conditions that have enabled the Internet economy to flourish? Governments are not alone in their efforts to protect children online. Parents, caregivers, educators, business and civil society can also help children to benefit from the Internet. They too have a responsibility to protect them against risks online.

Although some of these issues emerged in the early days of the World Wide Web, they have recently gained policy attention. At the Seoul Ministerial Meeting on the Future of the Internet Economy in June 2008, Ministers called for a collaborative effort by governments, the private sector, civil society and the Internet technical community to build a common understanding of the impact of the Internet on minors and to enhance their protection and support when using the Internet. They also called for increased cross-border co-operation by governments and enforcement authorities with respect to the protection of minors.

This report focuses on online risks for children and policies to protect them as Internet users. It examines direct and indirect policy measures available to OECD member and non-member countries to help mitigate risks for children online in order to:

- Present and compare existing and planned policy approaches for the protection of children online;
- Explore how international co-operation can enhance the protection of minors on the Internet.

Three broad categories of online risks for children are considered in this report: *i)* content and contact risks, including exposure to pornography, cybergrooming and cyberbullying; *ii)* consumer risks related, for example, to online marketing and fraudulent transactions; and *iii)* privacy and security risks, including the use of social networks without sufficient understanding of potential long-term consequences.

Statistical data about children's use of the Internet and the prevalence of risks are limited. The data are often fragmented and non-representative and offer few possibilities for comparing studies and countries. In particular, definitions of risks often differ, and survey methodologies vary significantly, making it difficult to compare risk prevalence rates. While the same spectrum of risks is present in all countries, the available data suggest that prevalence rates vary. Moreover, because children's activities, skills and resilience differ, their interactions with the online environment and the consequences differ as well. While children's capabilities are likely to increase with age, so can their own risky behavior.

Online risks faced by children are many and evolving. Addressing them requires a blend of approaches that include legislative, self- and co-regulatory, technical, awareness and educational measures, as well as

positive content provision and child safety zones. In practice, each country operates its own policy mix of characteristics and priorities, which reflects its perception of priorities as well as its culture and style of government. Moreover, policy measures that address different risks and initiatives from various stakeholders at different levels co-exist. This creates policy complexity at national level and policy heterogeneity across countries.

Government policies to protect children online are in their infancy. To enhance their efficiency and catch up with the rapid adoption of the Internet by children, governments face three main challenges:

- Managing policy complexity through enhanced policy co-ordination, consistency and coherence;
- Adopting an evidence-based policy-making approach;
- Taking advantage of international co-operation to improve the efficiency of national policy frameworks and foster capacity-building.

For policy to protect children online to operate effectively as the sum of its parts, governments should enhance the coherence of their policy measures and tools in collaboration with all stakeholders. Public-private partnerships, for instance, have been a successful way to encourage self- and co-regulation. Policies to protect children online would benefit from efforts to ensure consistency with other important policy objectives, such as the preservation of fundamental rights and maintenance of the framework conditions which have enabled the Internet to become a global open platform for innovation, economic growth and social progress.

With some notable exceptions, the impact of national policy frameworks and individual policy measures for the protection of children online is not regularly assessed and performance evaluations are only exceptionally built into policy. A systematic approach to evidence-based policy making is essential to determine policy priorities and maximise the protection afforded by national policy. The policy-making process would benefit from official statistics on children's use of the Internet and the prevalence of risk. This would require a more consistent approach to definitions, methodologies and indicators. Impact assessments would help address conflicting policy objectives and place greater emphasis on the quantification of benefits and costs.

International and regional co-operation is another area for improvement. While international and regional intergovernmental organisations (including, in addition to the OECD, the Asia-Pacific Economic Co-operation, the Council of Europe, the International Telecommunication Union, the Internet Governance Forum and the European Commission) are already involved, co-ordinated international work by governments and other stakeholders to protect children online would also support efforts by governments at national level.

Successful international co-operation relies on the involvement of all relevant international stakeholders. The report provides examples of international co-operation at the policy and operational levels. These include international strategic partnerships, capacity building and joint events (*e.g.* Safer Internet Day) as well as the sharing of successful educational and awareness raising campaigns. However, the organisation of a regular joint international event on child protection online, with the participation of national and international players, would be an effective way to co-ordinate efforts and take advantage of potential synergies. It would offer a way to share best practices among governments, business and civil society, including the research community, with a view to making the lessons learned from field experience available to policy makers. It would also help bridge communities such as policy makers and practitioners in the area of Internet policy, education, development and capacity building, law enforcement, and statistics.

Another avenue for international co-operation is the development of more comparable statistics to enable comparisons across countries and to help governments better assess the efficiency of their frameworks. OECD model surveys could, for example, include a module on children's access to and use of the Internet and on risk prevalence. Significant work would be needed to harmonise age ranges and define risks to determine data collection methodologies (*e.g.* survey of parents and educators *versus* survey of children).

PROTECTING CHILDREN ONLINE
Risks faced by children online and policies to protect them

INTRODUCTION

The Internet is an essential infrastructure for economic and social interaction. While it brings many benefits to all users, it also carries a spectrum of risks. Children can benefit greatly from the Internet. It is a significant tool for their education, creativity and self-expression as well as for the development of their identity and social skills. However, they are also more vulnerable to risks than adults. Governments, parents, caregivers, educators, business and civil society can help children to benefit from the Internet, but they also have a responsibility to protect them against risks online.

As the number of children using the Internet increases and the age at which they begin decreases, identifying and addressing these risks becomes an important public policy objective. Governments face many challenges when developing and implementing policies to protect children online: How to mitigate risks without reducing children's opportunities and benefits? How to prevent risks while preserving fundamental values such as freedom of speech and the right to privacy for all Internet users, including children themselves?

Some of these issues were raised at the OECD in the early days of the expansion of the World Wide Web.[1] Since then, the diffusion of broadband access and the exponential growth of available online content and applications over the last decade have significantly modified the landscape. At the Seoul Ministerial Meeting on the Future of the Internet Economy in June 2008, Ministers called for a collaborative effort by governments, the private sector, civil society and the Internet technical community to build a common understanding of the impact of the Internet on minors and to enhance their protection and support when using the Internet. They also called for increased cross-border co-operation on the protection of minors by governments and enforcement authorities (OECD, 2008).

This report builds on a Joint APEC-OECD Symposium on Initiatives among Member Economies Promoting Safer Internet Environment for Children held in Singapore on 15 April 2009 (OECD, 2009a)[2] and on APEC and OECD members' responses to a questionnaire on protection of children online. It is expected to contribute to work on the 30th anniversary review of the OECD 1980 Privacy Guidelines. It follows on the OECD Conference on Empowering E-Consumers held in Washington, DC, on 8-10 December 2009 (OECD, 2010c).[3] Its main objectives are to:

- Present and compare existing and planned policy approaches for the protection of children online;
- Explore how international co-operation can enhance the protection of minors on the Internet.

Countries' approaches to defining risks and prioritising policy responses vary with their culture, legal framework and style of government. For example, children's exposure to illegal or harmful content is defined and addressed in different ways, depending in part on each government's approach to free speech. Taking these differences into account, the report aims to identify areas in which efforts to co-operate, share experience and, as appropriate, minimise differences in policy and regulatory approaches may be valuable.

After a presentation of the scope of this report, of statistics on the use of the Internet by children, and of considerations regarding quantitative data on risks faced by children online, Parts I and II provide an overview of these risks and of policy approaches to addressing them. Policy findings are summarised in Part III. Annex I includes a detailed overview of current policy approaches. Annex II presents several tables and quantitative material on the prevalence of risk that support Part I.

Scope

The report focuses on OECD members, but also includes information on non-members.

Following the definition provided by the UN Convention on the Rights of the Child, Article 1, "a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier". Thus the category "child" (also referred to as "minor" in this report) may vary across countries and contexts. For example, under German media law, children are persons below the age of 14 and adolescents are persons as of age 14 but below the age of 18.[4] Protection often applies up to a specific age, sometimes less than 18 years, as under the US Children's Online Privacy Protection Act (COPPA) which protects personal data of children under 13.[5] National measures on child protection can also apply to minors at a higher age, as in Korea, where measures to protect children against harmful content apply to those under age 19.[6]

Risk mitigation strategies have to take account of the many factors that influence children's experience and activities on the Internet: the diffusion of Internet technologies or the socioeconomic situation of a given country's households (Hasebrink *et al*., 2009, p. 21, 57f.), the locations at which children most often access the Internet (*e.g.* home, school, public places, etc.) and the devices they use (*e.g.* computer, netbook, mobile phone, game console, etc.). This complex landscape varies among countries and is evolving rapidly. For example, with the diffusion of smartphones and other means to access the Internet (*e.g.* Internet dongles and 3G USB keys), ubiquitous Internet access may be on the rise among children as for adults. A brief overview of Internet use by children is provided below.

This report focuses on online risks to children. It does not address offline risks,[7] or crimes or issues related to online images of sexual abuse or sexual exploitation of children. However, online solicitation of children for sexual purposes – cybergrooming – where the risk starts online and then moves offline, is included. Ongoing work by the Council of Europe on criminal law issues related to online child sexual abuse and sexual exploitation will complement this OECD report by covering this other aspect of the subject matter. Arguing that full implementation of the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201) and of the Budapest Convention on Cybercrime (CETS 185) provides countries with adequate tools and mechanisms to deal with this issue, this work will be based on these legal instruments as benchmarks to assess how countries criminalise sexual violence against children.[8]

Although the report covers conduct by children that can create risks to themselves (or their parents), such as actively searching for explicit online content (Byron, 2008, p. 53), it does not cover online activities by children that can create risks for other children. For example, in the case of cyberbullying, the report focuses on children being bullied rather than on children who are cyberbullies, but it maintains the link to situations in which aggressors are victims, for instance peer-to-peer harm. Finally, pathological risks related to children's excessive use and overconsumption of Internet content or services are not within the scope of this report.

The report focuses on government policies to protect children online but it takes into account the essential role and shared responsibility of all stakeholders, in particular parents, caregivers and educators as well as business and civil society, and recognises that children are themselves essential stakeholders (see

Part II). The report examines direct and indirect policy measures and other means used by government to promote self- and co-regulation as well as private measures.

As the report covers a wide spectrum of risks, it does not provide a comprehensive analysis of each risk scenario or an inventory of all initiatives carried out worldwide to protect children. Rather, it provides a high-level overview of risks and efforts to address them across governments, business and civil society. It highlights commonalities and differences across countries with respect to policy measures and challenges. It is based on available research, on responses to the APEC Questionnaire on Children Protection Online circulated in April 2009 to APEC and OECD members,[9] and on direct input from OECD delegations and relevant experts.

Statistics on the use of the Internet by children

The following provides a quick overview of the use of the Internet by children, a topic that has been widely researched. It is based on a selection of reports. For example, in 2009, an inventory found 441 empirical studies from the European Union on children's access to and use of the Internet.[10] The fact that some countries are not covered in this section may reflect a lack of data on these countries and/or a bias in the selection of sources (*e.g.* language barrier). Children's access to the Internet is likely to be correlated with their country's Internet diffusion. It is important to note that children, like all Internet users, are affected by the digital divide. When they lack the opportunity to access the Internet, they cannot be affected by online risks; however, they also miss out on the opportunities and benefits the Internet offers.

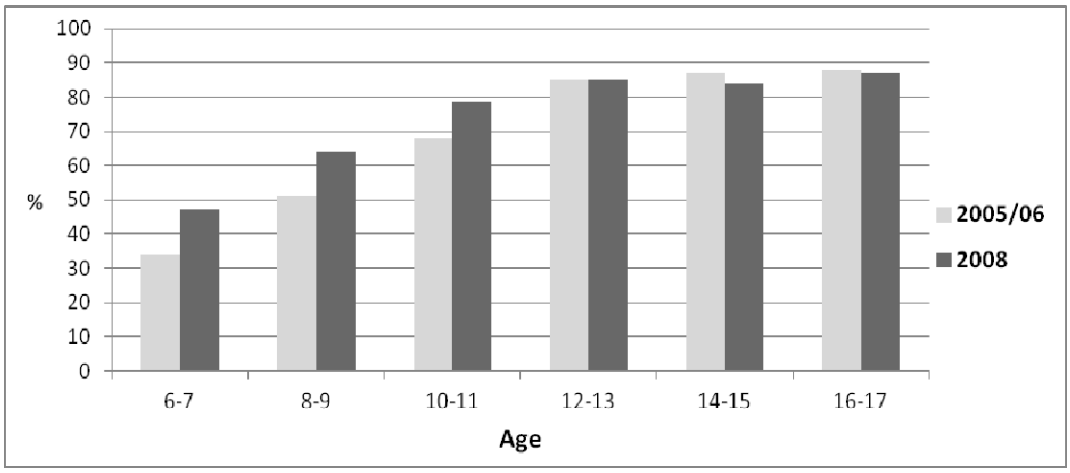
A review of the main studies available reveals several trends:

A high percentage of older children have Internet access: 93% of American children had access to the Internet in 2007 (Pew Internet & American Life Project, 2007, p. 48). In 2006 in Japan, this was the case of 65% of children aged 10-14 and 90% of teenagers aged 15-19.[11] In the European Union, 75% of 6-17 year-olds were reported by their parents in 2008 to use the Internet; the percentage ranged from 93-94% in Finland, Iceland and the Netherlands to 50% in Greece and 45% in Italy (Livingstone and Haddon, 2009, p. 111). Ofcom's research shows that 99% of UK children aged 12-15 use the Internet, 93% of 8-11 and 75% of 5-7 (Ofcom, 2010, p 3).

Internet access is on the rise: An increasing number of children have access to the Internet, mostly owing to the multiplication of computers in households and in schools. In the United States, 35% of public schools had access to the Internet in 1994 and 100% nine years later (Schmidt and Vandewater, 2008, p. 76); home Internet access for 8-18 year-olds nearly doubled over the last ten years (from 47% in 1999 to 84% in 2009) (Kaiser Family Foundation, 2010). The percentage of children using the Internet in the European Union increased from 70% to 75% over three years (2005-08) (EC, 2006, 2008c).

Internet use increases with age: In 2008 in the European Union, the Internet was used by 50% of 6-7 year-olds and 86% of 15-17 year-olds (EC, 2008c) (Figure 1). In Australia, a recent study showed that children aged 8 to 11 used the Internet on average 4.1 days per week for 1.3 hours per day, and that 12 to 17 year-olds used the Internet on average 6.3 days for an average of 2.9 hours per day (ACMA, 2009b, p. 8)

Figure 1. Children's Internet use by age in the European Union



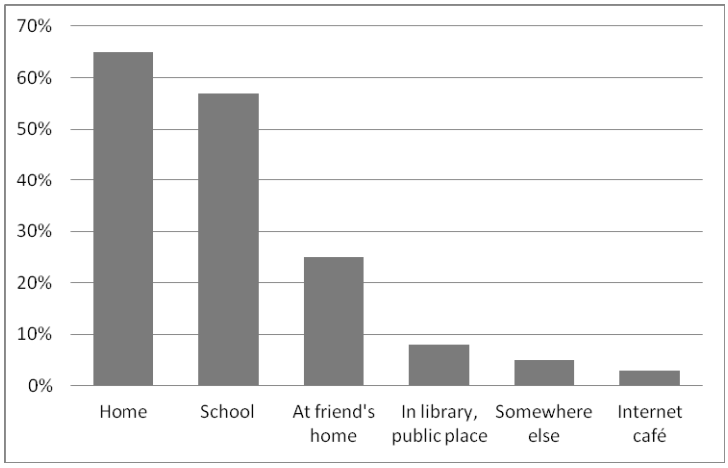
Source: OECD chart based on Eurobarometer 2005-2006 and 2008 (EU27).

Children start to use the Internet younger: A 2009 Swedish report points out that the age of Swedish children's first use of the Internet dropped from 13 years in 2000 to 4 years in 2009. The report considers that at least half of 4 year-olds use the Internet at least occasionally (Beantin Webbkommunikation, 2010). In 2009, 74% of British children aged 5-7 had access to Internet (Ofcom, 2010, p 16).

Children spend more time on the Internet than before: In 2007, British children aged 12-15 spent on average 13.8 hours a week on the Internet, nearly twice as much time as in 2005 (7.1 hours a week) (Ofcom, 2008c, p. 2). In 2003, Yahoo! commissioned a study indicating that Americans aged 13-24 already spent 16.7 hours a week on the Internet, *i.e.* more time than watching television (Yahoo! and Carat Interactive, 2003).

Children use the Internet mostly at home: 84% of children in the United States (Kaiser Family Foundation, 2010, p. 3) and 67% in Australia (Dooley *et al*., 2009) use the Internet at home. In the European Union, 65% of 8-17 year-olds access the Internet at home, followed by school and friends' homes (Figure 2).

Figure 2. European Union: Where does your child use the Internet? (8-17 year-olds)



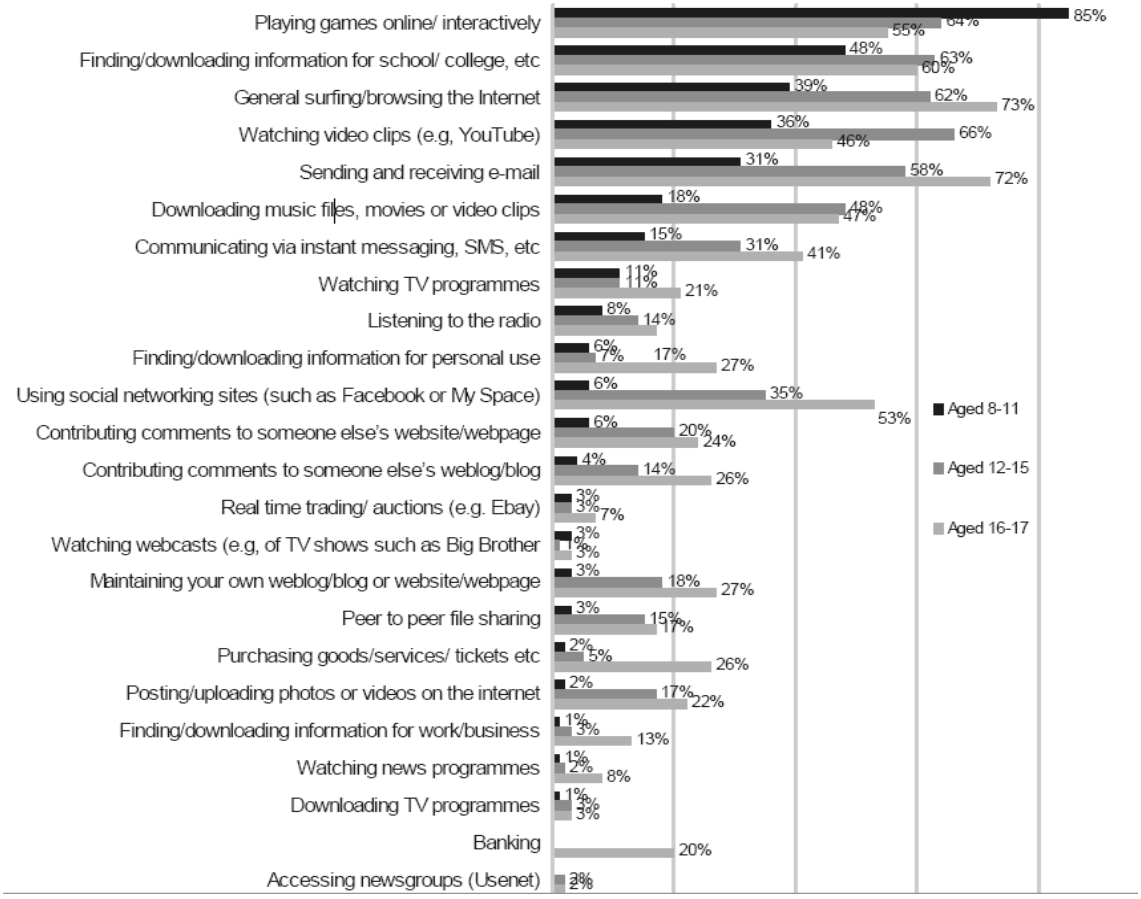
Source: EC, 2008c, p. 14, (EU27).

Children have a multitude of online activities which largely depend on age and changing usage trends. In 2007, the British communications regulator, Ofcom, provided a list of 24 activities carried out by children online and classified by age range (Ofcom, 2007, p. 19). Playing games was the most popular activity for children aged 8-11 but ranked fourth for children aged 16-17 after general surfing, sending and receiving e-mails and finding/downloading information for school. While 53% of 16-17 year-olds used social networking sites only 6% of 8-11 year-olds did so (Figure 3). Internet uses are extremely dynamic and trends in each type of use change rapidly. "Web 2.0" has modified Internet use by children, and the Pew Internet & American Life Project (2007, p. 47) mentions that use of chatroom decreased from 24% in 2001 to 18% in 2006. This likely reflects the fact that instant messaging functions are now an integral part of every social network or online community. In Australia in 2008, 90% of young people aged 12–17 reported using social networking services, with 51% of 8–11 year olds using these services (ACMA, 2009b, p.8). According to a recent US study (Kaiser Family Foundation, 2010, p. 21), visiting social networks has become the most popular activity among children aged 8-18.

Devices to access the Internet are diversifying: More sophisticated mobile phones increasingly enable Internet access (see Annex II, Table 1). Differences in Internet-enabled mobile phone usage by children across countries are important: nearly 60% of Japanese children use their mobile phone to access the Internet[12] but only 10.7% of European children (Eurobarometer, 2008c, annex tables and survey details) (Figure 5). It is likely that children will progressively make more use of Internet-enabled mobile devices in most OECD countries, following the Japanese example, depending on countries' socioeconomic conditions: for example, 14% of British children aged 12-15 used their mobile phone to access the Internet in 2009 (Ofcom, 2010, p 17). Moreover, the age at which children acquire their first mobile phone is dropping: the Pew Research Center's Internet & American Life Project, which tracks adolescent cell phone use confirms this trend: 58% of those aged 12 owned a mobile phone in 2009 while only 18% did in 2004 (Pew, 2009, p. 2). According to another Pew Internet research, 19% of 12-17 year-olds access the Internet through portable gaming devices (Pew, 2010). In 2009 in the UK, 12% of 5-15 years-old used their gaming console to access the Internet, rising up to 18% with children aged 12-15 (Ofcom, 2010, p 17). Children seem to access the Internet via mobile devices *in addition* to fixed computers rather than *instead* of them (Ofcom, 2010, p 9).

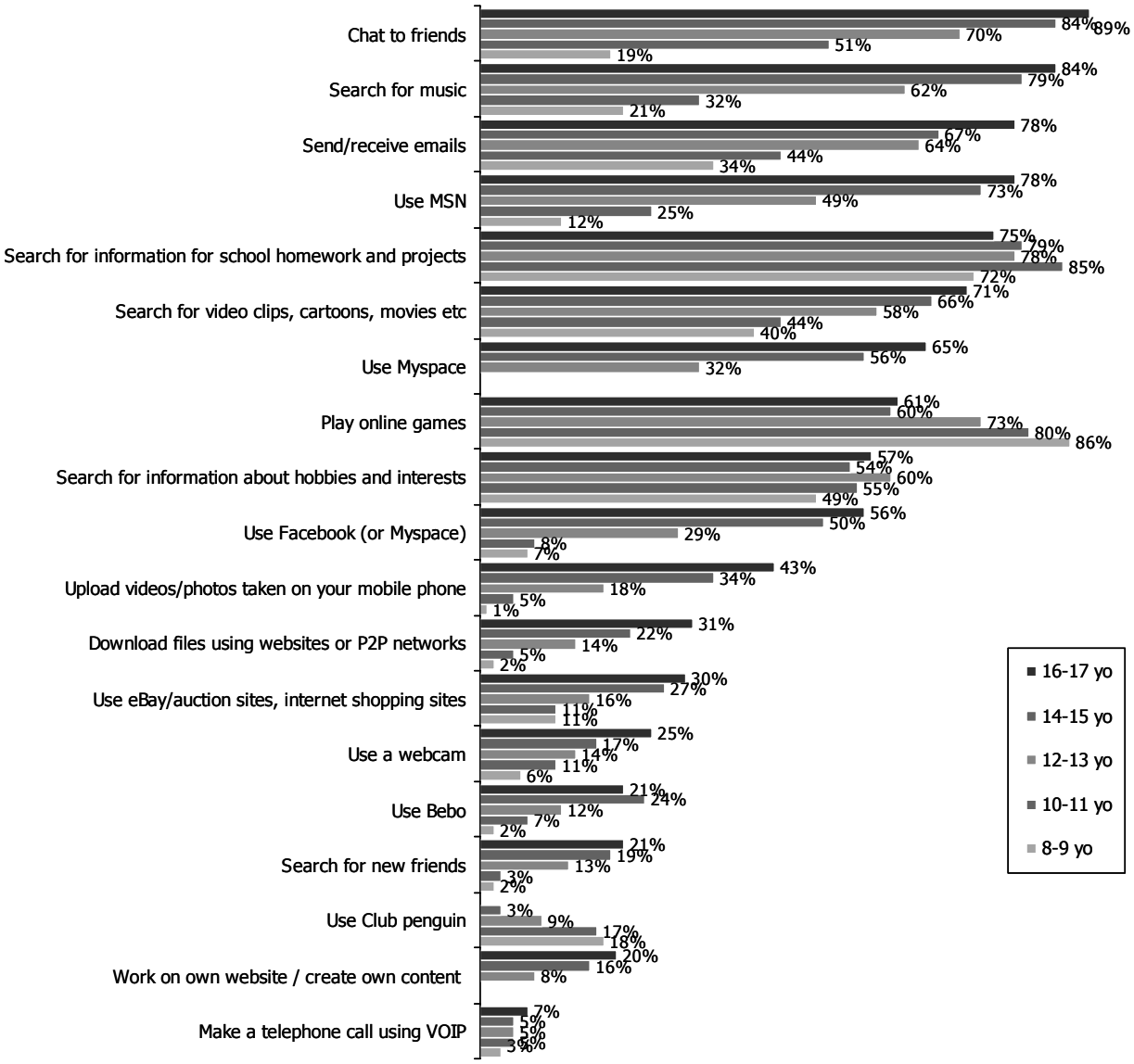
As regards the use of Internet filtering software, trends are not uniform across countries. For example, according to Marwick *et al.,* (2010, p.18-19) who compared studies carried out in 2005, 2007 and 2009, the use of filtering software in the United States increased from 44% to 56%. However, in the United Kingdom, Ofcom found a decrease in the use of control or filtering software by parents, from 49% in 2008 to 43% in 2009 (2010, p.4).

Figure 3. Children's use of the Internet by age group in the United Kingdom (2007)



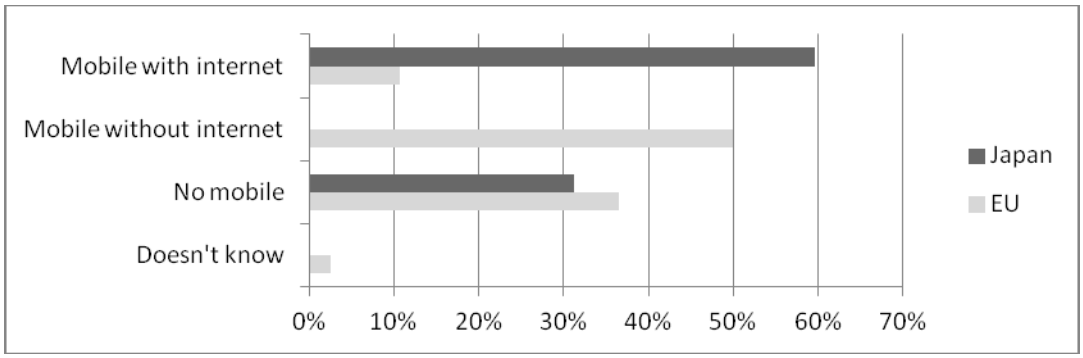
Source: Ofcom, 2007, p. 19.

Figure 4. Children's main reason for using the Internet by age group in Australia (2009)



Source: ACMA, 2009, p. 26.

Figure 5. Percentage of children owning a mobile phone with Internet access in Japan and the European Union, 2008



Source: Japanese delegation to the OECD and Eurobarometer 2008 (EU27).

Source: Pew Internet & American Life Project (2010), Social media and mobile internet use among teens and young adults.

In conclusion, a very high percentage of children have access to the Internet and general trends indicate that more children are going online and at an increasingly young age, are using a multitude of devices and are spending more time using the Internet. Understanding children's Internet usage patterns is a prerequisite for public policy-making in this area.

Considerations regarding statistics on risks faced by children online

A great deal of the empirical data on risks is available and will be reflected in the overview of risks in Part I. The availability and comparability of the data need however to be put into perspective. It is important to note that the current understanding of the prevalence of risk is based on a limited number of well-researched countries; for other countries, few data may be available. Risk prevalence varies and further comparative research would help to understand factors which influence differences among countries and regions.

Availability

The availability of quantitative data varies depending on the risk. There are few data on illegal interaction, harmful advice, online marketing to children, fraudulent transactions, information security risks and privacy risks. There is a great deal of data on exposure to inappropriate content (mainly adult pornography) and cyberbullying. Other risks are moderately addressed. The lack of data related to risks such as online gambling and overspending may be due to the methodological complexity of collecting the relevant quantitative data. The most studied risks are often those with the most serious immediate consequences, but they may not be the most prevalent. In general, studies focus on a limited set of risks which also attract the most media attention, *e.g.* exposure to pornography. Risks to privacy are less visible on the research agenda.

While at national and regional levels both quantitative (*e.g.* Eurobarometer) and analytical studies are widely available, this is not the case at the international level: quantitative, analytical and comparative studies are rare and not necessarily focused on children (*e.g.* Dooley *et al*., 2009).

The majority of studies explore a specific or a small number of risks (*e.g.* cybergrooming, exposure to pornography, etc.). Multi-risks studies generally emphasise cybergrooming, exposure to pornography and, to a lesser extent, exposure to violence and cyberbullying. Most research focuses on teenagers or young adults, and few data are available on younger children, even though they increasingly access the Internet. Most studies also focus on computer-based Internet access and do not take account of mobile Internet, which is increasing steadily and raising new issues. Finally, little research seeks to identify groups of children who might be more vulnerable to specific risks.

Studies rapidly become obsolete because of the evolution of online usage patterns and the technology landscape. For example, over the last 12 months, users have switched from chat applications to social networks as the latter implement instant messaging tools. Furthermore, the majority of available data are snapshots, and the lack of time series makes it difficult to evaluate trends.[13]

Comparability of data

Age: Age scale is a major challenge in data comparisons as age groups are not standard. Differences are striking when comparing national reports: for example, available data on exposure to violent content on the Internet in Europe ranges from 90% in Ireland for users aged 10-20, to 25% in Italy for children aged 7-11 (Annex II, Table 2).

Definition: There is a lack of consensus on the definition of risks. The variations in definitions, in particular of content risks such as pornography and hateful content, reflect differences in countries' cultural and social values. For example, the definition of "pornography" may range from semi-nude or nude pictures to explicit representation of sexual activity. As a consequence, risk prevalence rates are hardly comparable. Finally, different definitions can lead to the use of different measurement methods and thus affect prevalence rates and their comparability.

Selection of interviewees: As Figure 6 shows, results to the same question can vary tremendously depending on the respondents (parents or children). This may be because parents' knowledge of what their children do online is inaccurate, because children may be uncomfortable discussing subjects such as sexuality, and/or because of differences in perceptions about the inappropriateness of certain types of content.

In general, the conceptual framework of studies must be fully taken into account when interpreting these data.

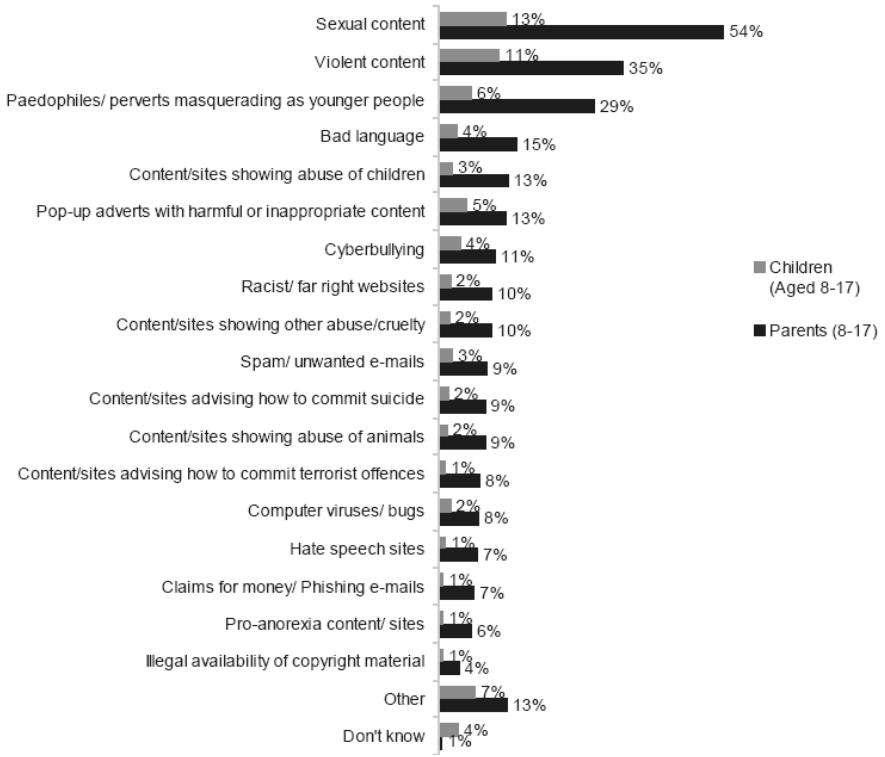
Conclusion

Empirical and analytical data on children's Internet use and exposure to online risks are widely available but highly fragmentary. In many instances, the data are not representative and offer few possibilities for comparisons of studies and countries. Basic alignments with regard to the age groups monitored, the definitions of risk, and the data sets on how children use the Internet would help to overcome some of these shortcomings.

Many countries do not yet undertake longitudinal surveys, with the result that observations over time on the evolution of risks are lacking, potentially hampering policy learning.

Data that enable comparative analysis of the prevalence of risk across countries would foster common understanding of national and regional trends in risks for children online, help develop effective national policies and facilitate international co-operation.

Figure 6. Concerns about content on the Internet – type of material: parents *vs.* children's perception in the United Kingdom



Note: children who expressed concerns about content on the Internet were asked "What sort of things are you worried about?". Parents who expressed concerns about content on the Internet were asked "What sort of things are you worried about for your children?"

Source: Ofcom, 2007, p. 72.

PART I. ONLINE RISKS FOR CHILDREN

Typologies of risks

Risks to children online reflect the broad spectrum of children's use of the Internet. Several classifications of risks have been developed by the US Internet Safety Technical Task Force (ISTTF) and the US Online Safety and Technology Working Group (OSTWG), the Australian Communications and Media Authority (ACMA), EU Kids Online, the European Youth Protection Roundtable Toolkit (YPRT) and the International Telecommunications Union (ITU) Guidelines for Policy Makers of Child Online Protection (2009a). While each of these classifications reflects the particular approach taken by these studies, they all distinguish between risks related to harmful content and those to harmful interactions.[14] However, other classification criteria vary. For example, the EU Kids Online report includes a complex risk matrix that takes into account the role of the child (whether she/he is the initiator of the risky interaction) and the nature of the risk (commercial, aggressive, sexual and values-related); Australia includes e-security risks such as viruses and online fraud which are not covered by the EU Kids Online report.

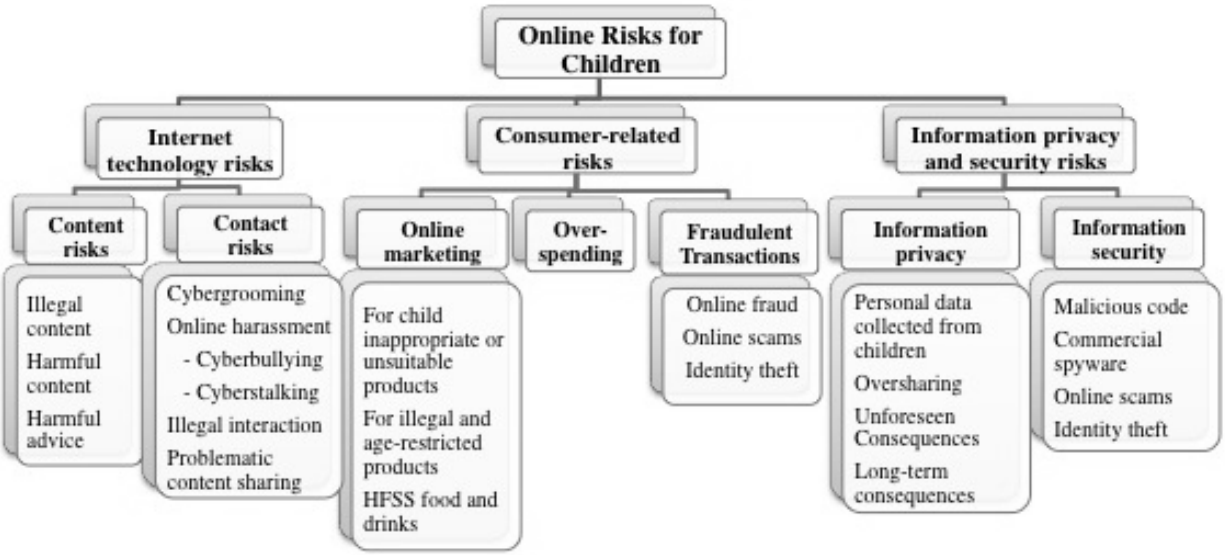
Several additional criteria can be used to classify risks, including whether: *i)* the child is interacting with a human (*e.g.* cybergrooming) or a machine (*e.g.* collection of personal data, gambling); *ii)* the risky interaction takes place between children (*e.g.* as is often the case with cyberbullying) or between a child and an adult (*e.g.* cybergrooming); *iii)* the online risk is an extension of a known offline risk (*e.g.* exposure to pornography) or specific to online contexts (*e.g.* illegal downloading); *iv)* only children are concerned by the risk or it is a general online risk and children are a particularly vulnerable user group (*e.g.* malware, privacy); and *v)* according to the devices children use (*e.g.* computer, mobile phone, etc.). Age, as well as the degree of maturity or resilience, can also be key criteria. Finally, risks can be classified according to their criminal dimension: those that do not have a criminal dimension, those for which the child is a potential victim of a criminal offence committed by a third party, and those for which the child commits a criminal offence.[15]

Overview of risks

Building on common elements of existing classifications and focusing on OECD Working Party on Information Security and Privacy (WPISP) and Committee on Consumer Policy (CCP) expertise, this report considers three broad categories of online risks for children: *i)* Internet technology risks, *i.e.* when the Internet is the medium through which the child is exposed to content or where an interaction takes place; *ii)* consumer-related risks to children online; *i.e.* the child is targeted as a consumer online; and *iii)* information privacy and security risks, *i.e.* risks every Internet user faces but for which children form a particularly vulnerable user group.

It is important to note the interplay among the risk categories. For instance the risk of exposure to content inappropriate for children stemming from online marketing involves two risk categories. Commercial risks may also involve privacy risks. In consequence, as definitions of risks used in official documents and the literature vary significantly, this report relies on the most common understanding of each risk category.

Figure 7. Typology of risks



Based on an overview of the risks (Figure 7), this section provides quantitative information gleaned from selected studies and reports in order to gauge the current size of the problem. It aims to provide a good understanding of the risk context but does not claim to be comprehensive. Given the nature of the literature on online risks faced by children, including quantitative data, consolidation of such information is difficult. Initiatives such as the Review of Existing Australian and International Cyber-Safety Research (Dooley *et al*., 2009) and the EU Kids Online study provide an in-depth inventory of existing research and have been extensively used here.

Risks pertaining to children as Internet users

Today's children are often referred to as "digital natives" because they grow up with the Internet. When they have the opportunity, children are keen Internet users. With over a trillion unique web pages in 2008,[16] children can be exposed to a vast variety of content. Interactivity is also a fundamental characteristic of the network. As a consequence, risks pertaining specifically to children as Internet users comprise *content* risks (the child passively receives or is exposed to content available to all Internet users in a one-to-many relationship) and *contact* risks (the child is actively involved in a personalised relationship or interaction, whether bilateral or multilateral).

Content risks

Content risks comprise three main sub-categories: *i)* illegal content; *ii)* age-inappropriate or harmful content; and *iii)* harmful advice. Potential consequences vary with the risk and other factors, such as the child's age and resilience.

Illegal content, *i.e.* content that it is illegal to publish, varies across jurisdictions. For example, promoting bestiality, racism, hate speech and other forms of discrimination may be illegal in some countries but not in others, where it might fall under the more flexible category of "age-inappropriate content" as described below. Content associated with sexual exploitation of children, however, is illegal in most countries, although the frequency of children's exposure to such content, while not known, is likely to be very low. In an American survey carried out in 2006, only two children aged 10-17 out of 1 500 had

come across such content, one of whom specified that it was through a misleading link (Wolak *et al*., 2006, p. 30).

Age-inappropriate content such as hate, violence or adult pornography, although generally not illegal, may harm children and their development. Children can accidentally stumble upon such content, can be referred to it by peers or can deliberately look for it. They can also engage in interactive media, such as online video games featuring realistic violence. Such content can be provided commercially but it is also often freely available or can be generated by Internet users. Internet material available to the general public is often not sensitive to the special situation of child audiences. Indeed, content which is harmful to minors sometimes even targets children, for example through misleading domain names. Web pages advocating hatred have also been found to contain sections for children, with games and misinformation targeted to them (Dooley, 2009, p. 106).[17]

> 4.5% of extremist right-wing websites studied in the United States in 2000 had sub-sections targeting children and young adults. "These sites often had colourful images, hate-filled games, and messages aimed at a preteen audience." (Shafer, 2002)

The definition of age-inappropriate content is likely to reflect national or regional cultures and societal values. Deliberations on the subject are often informed by traditional television regulation (Millwood Hargrave, 2009, p. 7) and public concerns tend to focus on pornography and sexually explicit content (De Haan and Livingstone, 2009). Substantial reviews of the evidence on the prevalence of risk and the consequences of children's exposure to certain categories of age-inappropriate content, such as pornographic and violent content, are available for a number of countries (ISTTF, 2008; Dooley *et al.*, 2009; Hasebrink *et al.*, 2009; Media Awareness Network, 2005; Grimm *et al*., 2008).

> On the Internet, children's accidental exposure to pornographic content increases when the names of problematic websites are modelled after popular children's websites (*e.g. www.teltubbies.com* was shut down in 2003 for misleading children). The National Center for Missing & Exploited Children's CyberTipline has maintained information on misleading domain names since it opened this category in 2000.[18]

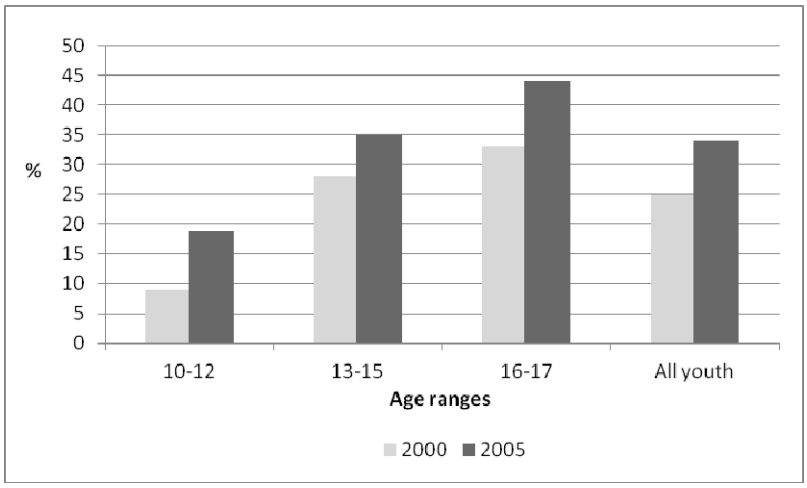
For example, prevalence rates vary depending on the definition of pornography. If nudity is considered pornography, they are likely to be higher than if pornography is defined as an explicit representation of sexual activity. Moreover, the notion of pornography is likely to vary not only across countries but also across communities or groups within a country. Finally, the age ranges vary considerably across studies and countries, so that comparisons would not be representative.

If sexuality is more openly discussed in the society, children may be more likely to admit having viewed nudity (Peter *et al.*, 2006, cited in ISTTF, 2008, Appendix C, p. 30 and in Dooley *et al*., 2009, p. 93). More generally, surveys that cover exposure to nudity and/or pornography may be subject to bias since they rely on children's voluntary expression regarding sexuality, a sensitive topic among adults and even more so among teenagers.

While it is recognised that pornographic material is relatively easy to find on the Internet, some research indicates that younger children are more exposed to pornography offline (*e.g.* films and magazines) than online (Dooley *et al*., 2009) and that this particular online risk may be somewhat overstated. In any case, there seems to be agreement that exposure to pornography online increases with

age (Figure 8), is more frequent among older male adolescents (ISTTF, 2008, p. 19) and that accidental exposure is more frequent than deliberate exposure. For example, a study carried out in 2006 in the United States found that out of 42% of 10-17 year-olds youth who reported exposure, 66% specified that it was unwanted (Wolak *et al*., 2006, cited in ISTTF, 2008, Appendix C, p. 30). Children who report having deliberately searched for pornographic sites seem to be mainly males (83% of boys and 17% of girls) (Wolak *et al*., 2006, p. 54).

Figure 8. Unwanted exposure to sexual material by age group (United States)



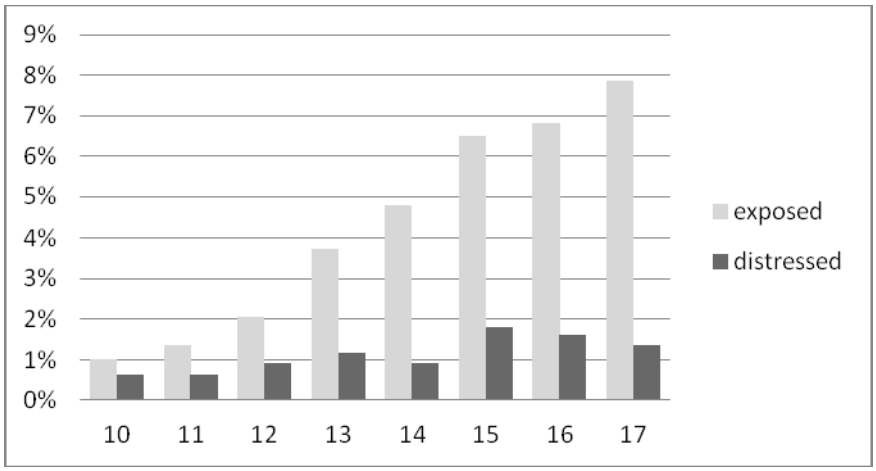
Source: Wolak *et al*., 2006, p. 8-9.

Some studies suggest that rates of unwanted exposure also increase with age and that the number of children exposed to pornography online has increased over time. According to a national study (Wolak, *et al.,* 2006), the percentage of young American Internet users seeing unwanted sexual material online increased from 25% in 2000 to 34% in 2005 (Figure 9) even though parents used more filtering, blocking and monitoring software (55% in 2005 compared to 33% in 2000). However, a survey that measured the impact of exposure to pornography on 10-17 year-olds found that relatively few children were distressed: of the 34% who reported having seen pornographic content online, only 9% reported being "very or extremely upset". The same study stresses that younger children are more likely to be distressed (Figure 9). Between 2000 and 2006 both exposure and impact seem to have increased (see Annex II, Figure 14).

The degree of children's exposure to violent content on the Internet is unclear and would benefit from further research. Few studies assess the frequency of exposure to violent content in the United States (ISTTF, 2008, p. 19) and Australia (Dooley *et al.*, 2009, p. 100), while European estimates range from 15% to 90% (see Annex II, Table 2). However, these estimates merge hateful and violent content and use different age ranges, thereby making it difficult to compare European countries.

Harmful advice can result in suicide, consumption of drugs or alcohol, or the development of eating disorders (*e.g.* anorexia). As anyone, including minors, can place such content on Web 2.0 platforms, it is particularly difficult to control. As information on these topics can also be well intentioned or mix well-intentioned with potentially harmful advice, it is difficult to draw the line between harmful advice and harmless or even useful advice (Millwood Hargrave *et al.*, 2009).

Figure 9. Unwanted exposure to sexual material by age in 2005 in the United States (n = 1 500)



Note: out of 1 500 children aged 10-17 surveyed, 512 (34%) experienced exposure and 136 (*i.e.* 9% of the total population surveyed or 26% of exposed children) felt distressed. Exposure increases with age but the proportion of distressed children diminishes accordingly.

Source: Wolak *et al*., 2006, p. 36.

Very limited data are available on risks related to online exposure to harmful advice. None were found on harmful advice related to suicide or drugs. Some research suggests that females are at higher risk for anorexia and self-injury. An American study found over 400 self-harm bulletin boards which shared information on the most effective self-harm techniques.[19] Users were found to be predominantly female aged between 16 and 23, most of them around 18 years old, and thus not always children as defined in national law. An Australian study found that the participants in a self-harm discussion group were mostly female (mean age of 21.4) and had begun self-harming at age 13.6 (Murray and Fox, 2006, in Dooley *et al.*, 2009, p. 125).

Contact risks

Contact risks occur when children interact online, for example when participating in online chats. They can be further distinguished according to whether: *i*) the interaction takes place with the intention to harm the child (*e.g.* cybergrooming); *ii)* children are exposed to hateful online interactions; or *iii*) the child inflicts harm to himself or herself by his or her conduct (*e.g.* liability due to illegal filesharing).

Cybergrooming, the use of the Internet by an adult to form a trusting relationship with a child with the intent of having sexual contact, is a criminal offence in several countries. This is in line with the provision of the Convention of Council of Europe on the Protection of Children against Sexual Exploitation (CETS 201) which criminalises sexual solicitation.[20]

> "Stranger danger" is a term coined to highlight the possibility of threatening contact from unknown adults, particularly sexual predators, (Byron, 2008, p. 53) not only on the Internet. Chatrooms, where contact with strangers can occur more easily, seem to be especially risky (Dooley *et al.*, 2009 p. 53). Obviously, not all strangers present a danger.[21]

There has been a good deal of research on cybergrooming. However, quantitative data are limited to a few widely cited studies, such as Wolak's, which are referred to in most of the relevant international literature. The general conclusion appears to be that minors are only exceptionally abused by adult predators who contacted their victim online and lied about their age, identity or intention to have sexual contact offline (Dooley *et al*., 2009, p. 29). The reality of cybergrooming seems more complex. It may certainly begin with a misrepresentation of the adult's true age to a child in order to begin to engage the child's affections. However in most cases, there is no deceit of any kind at any stage in the online or offline relationship, which sometimes involves young adults or legal minors (Dooley *et al*., 2009, p. 29). This does not minimise the responsibility of an adult who takes advantage of a child's naiveté, but it does indicate a need for a more sophisticated understanding of how to tackle or prevent such situations from occurring.

The concept of "sexual solicitation" can be interpreted differently. A flirty comment can be regarded as such by some and not by others. Research suggests that minors are at limited risk of receiving "sexual solicitations" from unknown adults. According to Wolak *et al.,* 2006, 25% of young people interact and share information with strangers online but only 5% have talked to a stranger online and discussed sexuality (Wolak *et al.*, 2006, and Ybarra *et al.*, 2007, cited in Dooley *et al.*, 2009, p. 48). Most tend to deflect or ignore sexual solicitation and to take appropriate steps in response. Between 43% and 48% of sexually related solicitations appear to come from adolescents and 20% to 30% from young adults under 21, but only 4% to 9% from adults (Dooley *et al.*, 2009, p. 10). Most seem to be made through chat rooms and instant messaging; the rise of social networks does not seem to have increased the phenomenon. Finally, there is some indication that the percentage of youth who receive sexual solicitations online declined from 19% to 13% between 2000 and 2006 (Finkelhor *et al.*, 2000; Wolak *et al.*, 2006, cited in ISTTF, 2008).

Physical sexual contact with an adult encountered online is very rare. Only eight youths out of 1 500 (0.5%) reported physical sexual contact in a 2005 American national survey (Ybarra *et al.*, 2007, p. 21) and all were 17 year-olds who had a relationship with young adults in their early twenties. Out of the 183 case files reported by the Pennsylvania Attorney General between 2005 and 2009, eight incidents (4%) involved teen victims with whom a relationship was formed on the Internet, 12 (6%) reported predators being deceptive about their age, 166 (90%) were police stings resulting in arrests, 87% of which took place in chatrooms.[22] This last figure suggests that the cybergrooming risk does exist but is difficult to measure precisely. Females represent 70% to 75% of victims and are more at risk; 99% are aged 13 to 17 (Wolak *et al.*, 2004, 2006, cited in Dooley *et al.*, 2009, p. 15, 21), perhaps because they tend to engage in the riskiest behaviour and are most likely to communicate with strangers online, although teenagers typically do not interact with strangers (75%) (Wolak *et al.*, 2006, and Ybarra *et al.*, 2007, cited in Dooley *et al.*, 2009, p. 52). Offline victims of an online approach under age 12 seem to be extremely rare.

Online harassment is arguably the most prevalent contact risk faced by children. It ranges from intimidation, embarrassment and humiliation to severe threats delivered via electronic means (ISTTF, 2008, p. 18; Millwood Hargrave *et al.*, 2009, p. 8). It can culminate in *cyberbullying*, whereby individuals or groups use information and communication technologies deliberately and repeatedly to harm others (ENISA, 2007, p. 15; De Haan and Livingstone, 2009, p. 5; Dooley *et al.*, 2009, p. 61). Although cyberbullies and their victims are often minors, cases of adults harassing children also exist. Strategies include repeated threats by e-mail, text messages or chat, publication on the web or circulation of embarrassing pictures, often taking advantage of the relative anonymity of the online media, although most victims know the identity of the person harassing them (ISTTF, 2008, p. 17; Dooley *et al.*, 2009, p. 11). "Flaming" is a form of cyberbullying in which children have an unusually intense and verbally aggressive argument via e-mail or instant messaging. In such interactions, aggressors and victims are generally children. As Figures 10 and 11 show, mobile phones and e-mail are the primary vectors of these types of harassment.

> "Cyberstalking" is a type of online harassment in which a single individual's conduct is an extreme form of online pursuit involving repeated contact and malicious threats; he/she may also compromise the victim's personal details in order to cause psychological and physical distress.

Online harassment and cyberbullying seem to be a growing area of concern (Cross *et al.*, 2009, and Wolak *et al.*, 2007, cited in Dooley *et al.*, 2009, p. 64). The prevalence of cyberbullying varies considerably. Older children are more at risk. There is also a correlation with the diffusion of Internet access and the availability of mobile phones among youth (Hasebrink *et al.*, 2009, p. 91 f.; Dooley *et al.*, 2009, p. 67 f.).

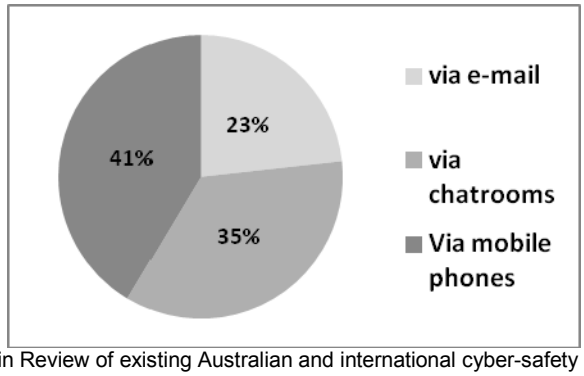
In spite of the large amount of available data on the prevalence of risk, it is difficult to compare prevalence rates. These range from 4% to 46%, owing to the different definitions in studies or in countries (Hinduja and Patchin, 2009; Kowalski *et al.*, 2007; Pew Internet & American Life Project, 2007; McQuade and Sampat, 2008; Smith *et al.*, 2008; Williams and Guerra, 2007; Wolak *et al.*, 2006; Ybarra *et al.*, 2007a, cited in ISTTF, 2008, p.17). For example, the most common definition of cyberbullying simply adds use of information and communication technologies to bullying, a form of harassment generally involving aggressiveness, intent to harm, repetition and a power imbalance between the bully and the bullied (ISTTF, 2008, p. 17; Finkelhor *et al.*, 2010). However, studies sometimes only consider three of these criteria or add another. The prevalence rates reported in Table 1 should therefore not be directly compared.

Table 1. Cyberbullying prevalence rates across countries

	Low prevalence rates	High prevalence rates
Australia	6.6% from year 4 to 9 in 7 500 schools	21% of 652 young persons aged 11-17
United States	11% of grade 6-8	50% of teens aged 13 to 18 were cyberbullied
Canada		55% of student aged 12 to 15
China		65% aged 11 to 14
United Kingdom	22% aged 11 to 16	
Europe (See Annex II, Table 4)	Iceland with 15% of 9-16 year-olds	Estonia with 31% of 6-14 year-olds

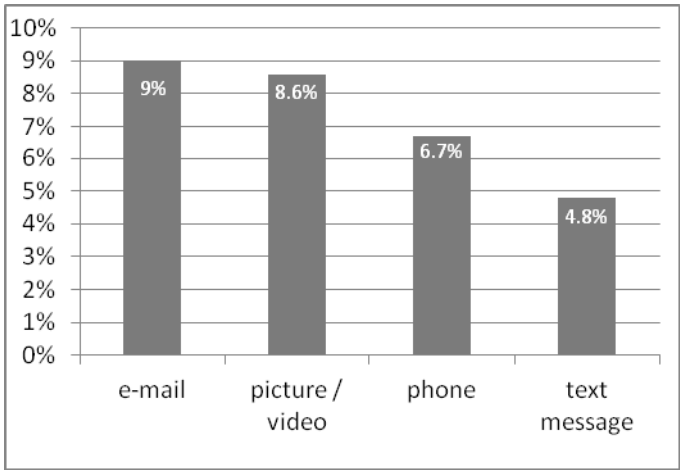
Source: adapted from Cross *et al.,* 2009, Lodge *et al.,* 2007, Kowalski *et al.,* 2007, Raskauskas *et al.,* 2007, Li, 2008 cited in Dooley *et al.,* 2009, p. 64-68, and EU Kids Online, 2009, p. 29.

Figure 10. Cyberbullying medium for middle school students in Canada in 2009



Source: Li, 2007a, cited in Review of existing Australian and international cyber-safety research (2009), p. 69.

Figure 11. Cyberbullying of Swedish students aged 12-15 in 2008 by medium



Note: This chart shows the percentage of students aged 12-15 in Sweden bullied via e-mail, picture/video, phone and text message.

Source: Slonje and Smith, 2008 cited in Dooley *et al*., 2009, p. 69.

According to several authors, offline bullying is twice as prevalent as cyberbullying (Li, 2007b, cited in ISTTF, 2008). Nevertheless, one study shows that 42% of children bullied online appear to also be victims of school bullying, an indication that the two are related (Hinduja and Patchin, 2009, cited in ISTTF, 2008, Appendix C, p. 22). Current research also suggests that:

- Minors are almost exclusively harassed by other minors and up to 82% of the victims know the identity of the aggressor (Hinduja and Patchin, 2009, cited in Dooley *et al.*, 2009, p. 71).

- Cyberbullying follows an inverse U-pattern, increasing with age until about the mid-teens when it peaks and then decreases (Kowalski and Limber, 2007, and Slonje and Smith, 2008, cited in Dooley *et al.*, 2009, p. 75). In Australia, cyberbullying is reported by 1% of 8-9 year-olds but up to 19% of 16-17 year-olds, only to decrease after (ACMA, 2009b, p. 63).

- The impact of online harassment is relatively strong. For example, an American study found that 39% of victims reported emotional distress (ISTTF, 2008, p. 17).

- E-mail and mobile phones seem to be the most common sources of cyberbullying (see Figures 10 and 11). Online harassment occurs mostly while using instant messaging or visiting chat rooms (Kowalski and Limber 2007; Opinion Research Corporation, 2006a, 2006b; Wolak *et al*., 2006, cited in ISTTF, 2008, Appendix C, p. 46-47).

- There seems to be a gap between children's and parents' perceptions. For example, while 33% of UK youths aged 9-19 reported online harassment, only 4% of parents believed that their children encounter online harassment (Livingstone and Bober, 2004, cited in ISTTF, 2008, Appendix C, p. 44).

- Cyberbullying is sometimes related to privacy and identity theft (see below).

- Some children who participate in cyberbullying, for example by forwarding pictures or messages to others, do not always fully realise the effect of their conduct on the victim. Evidence on this topic is lacking.

Children are most likely to encounter *hateful speech in live interactions* between players in videogames, in chat rooms and in virtual worlds.[23] In a 2008 American Pew Review, nearly half of game-playing teens reported seeing or hearing "people being hateful, racist or sexist while playing" at least sometimes, and 63% reported "people being mean and overly aggressive" (Lenhart *et al*., 2008, cited in ISTTF, 2008; Dooley *et al.*, 2009, Appendix C, p. 50). A small-scale US-based study in 2004 reported that chat participants had a 59% chance of exposure to negative racial or ethnic comments during an unmonitored interaction (Tynes *et al.*, 2004, cited in Dooley *et al.*, 2009, p. 107). Another noted that 51% of teenagers reported never seeing or hearing "people being hateful, racist or sexist while playing", 33% reported this happening sometimes and 16% "often" (see Annex II, Table 4).

Minors in search of help or assistance can receive *harmful advice* from incompetent or ill-intentioned advisors on interactive platforms such as social networks or chat rooms. This contact risk mirrors the risk of being exposed to harmful advice in static content. While the interaction with a group of like-minded users can normalise and reinforce dangerous practices such as self-harm or anorexia (Dooley *et al.,* 2009, p. 125, 129), some dedicated online sites discuss these problems, and members offer support rather than harmful advice. Others mix constructive and harmful views, making distinctions difficult.

In *sharing of problematic content* (ISTTF, 2008, p. 19) children create problematic content, most often using a camera phone or webcam, and then post and share it online. In this category belong images or videos portraying group or self-inflicted violence and "sexting*"*, a practice in which minors forward nude or semi-nude photographs of themselves (ITU 2009a, p. 33; Pew Internet & American Life Project, 2009, p. 4).

"Dedipix*"* is a recent trend, apparently initiated in France (Cosgrove, 2009), whereby children post a picture of one of their body parts, sometime nude or semi-nude, with a message written on it. This cuts across several risk categories, as it contributes to the presence of harmful or even illegal content and once in the public domain poses both a short-term and a long-term threat to the child's privacy (Pew Internet & American Life Project, 2009, p. 5f.; Solove, 2007, p. 2). So-called "happy slapping*"* refers to an assault, usually on a stranger, by teenagers either "just for fun" or as part of a deliberate assault or robbery while someone films the action with a cell phone camera. The videos are then posted on video-sharing platforms or exchanged via mobile phones.

Data available on such risks are limited. In an American national survey published in 2007, 4% of youths who use the Internet reported they had received a request for a sexual picture of themselves but only one in 1 500 complied (Mitchell *et al.*, 2007c, cited in ISTTF, 2008, Appendix C, p. 51). According to a US regional study, 7% of students in grades 7–9 had received an online request for a nude picture (McQuade and Sampat, 2008, cited in ISTTF, 2008, Appendix C, p. 51). A study carried out in Iceland found that 15% of teenagers reported having asked other teenagers online for a picture of themselves naked (Hasebrink *et al.*, 2009, p. 30). However, it is unclear whether this represents private communications between two teens and/or posting to a wider audience.

Other data show that problematic content may be more frequently shared via a cell phone than online. A recent American study found that 4% of youths aged 12-17 who owned cell phones had *sent* sexually suggestive nude or nearly nude images of themselves to someone else via text messaging, 15% said they had *received* sexually suggestive nude or nearly nude images of someone they know, 8% reported *being a victim* of images transmitted over a cell phone. The likelihood of sending or receiving such content seems to increase with age: 4% of 12- year-olds reported having received such images or videos compared to 20% of 16 year-olds and 30% of 17 year-olds (Pew Internet and American Life Project, 2009, p. 2). Interestingly, those who pay their own phone bills are more likely to send these images than those who do not (17% and 3%, respectively).[24] This is probably age-related, *i.e.* more 17 year-olds may pay their bill than 13 year-olds.

Illegal interactions can place minors or their parents at risk of criminal or civil penalties. For example, online piracy or sharing copyrighted material can, in some jurisdictions, such as France, lead to legal proceedings or put the household's Internet access at risk of being suspended. *Online gambling* by minors, which is illegal in most countries, is a financial threat to parents if minors have access to a credit card or other means of payment such as a mobile phone. It is also a potential source of psychological harm to the child concerned.

Although illegal file-sharing is often associated with teenagers, there are no data specifically on file-sharing activities of children. Data on children's use of gambling websites, an illegal activity in many countries, are lacking, but the "UK Children Go Online Survey" reported that 2% of minors admitted to having gambled online daily/weekly (Livingstone and Bober, 2005).

Children targeted as consumers on the Internet

Children face consumer risks online when *i)* they receive online marketing messages that are inappropriate for children (*e.g.* for age-restricted products such as alcohol); *ii)* they are exposed to commercial messages that are not readily identified as such (*e.g.* product placements) or that are intended only for adults (*e.g.* dating services); or *iii)* their credulity and inexperience are exploited, possibly creating an economic risk (*e.g.* online frauds).

Online marketing to children

Online advertisements for regulated or age-restricted products to minors such as alcohol, cigarettes and prescription medicines raise concerns that such marketing downplays risky lifestyles and links children to suppliers online. The possibility for children to buy age-restricted products online does not necessarily mean that they do so. For example, an American study in 2006 indicated that over 70% of teenagers who tried to purchase cigarettes online succeeded, and another from 2002 found that only 2.2% of 1 689 teenagers who smoked bought their cigarettes online (Dooley *et al.*, 2009, p 133) The *promotion and sale of illegal products* such as drugs and doping substances on the Internet present a risk primarily for adolescents (US Department of Justice, 2002, p. 1).

Online marketing targeting children or displayed on a webpage popular with children can be problematic when there is a *lack of separation between content and advertisement*. For minors, particularly younger children, commercial content is less distinguishable from other content and their ability to critically engage with advertising messages is less developed;[25] this leaves them more vulnerable to the influence of online marketing (Fielder *et al.*, 2007, p. 11; De Haan and Livingston, 2009, p. 5; OECD, 2010b, p. 7). "Advergaming" is an example of a controversial marketing technique which mixes advertising with online games or videos (Kaiser Family Foundation, 2006, p. 5f.). Children have insufficient understanding of how Internet content is produced and financed, which is also a reason why they have difficulty critically assessing advertising messages (De Haan and Livingstone, 2009, p. 5; Fielder *et al.*, 2007, p. 12; UK Department for Children, Schools and Families, and Department for Culture, Media and Sport, 2009, p. 88; Media Awareness Network, 2005, p. 16). For this reason, some advocates have questioned the use of embedded advertising and commercial branding on websites that target children (UK Department for Children, Schools and Families, and Department for Culture, Media and Sport, 2009, p. 85). They have also raised the issue of whether or from which age children should be subjected to full-fledged online marketing practices.

Marketing/advertisement can harm minors by *including age-inappropriate content* to which children can be exposed in their daily use of the Internet (*e.g.* banners or spam e-mails containing sexually explicit images). The promotion of gambling and dating services can trigger minors' curiosity (Fielder *et al.*, 2007,

p. 11, 14, 18) and foster risky behaviour which might lead to financial loss or set the scene for sexual solicitation.

A study by the British National Consumer Council (now Consumer Focus) and Childnet International of commercial activities on websites favoured by children shows that 9% of the ads are for online gambling and 4% for dating services (Fielder *et al.*, 2007, p. 11). In one study, pornographic pop-up advertisements are the primary reason for children accidentally stumbling over explicit content while doing something else online (Livingstone and Bober, 2005).

Internet marketing of food and drink products that are high in fat, sugar and salt (so called HFSS food) may affect the risk of childhood obesity. This issue is under public scrutiny in many countries (Fielder *et al.*, 2007, p. 11).[26] Policy makers in some countries have expanded or are considering expanding existing regulations or self-regulatory measures on the marketing of such products on television to cover websites targeting children (UK Department for Children, Schools and Families, and Department for Culture, Media and Sport, 2009, p.105).

Overspending

Overspending on online or mobile services by minors can generate *high costs* for parents (OECD, 2006, p. 8). For example children can subscribe to fee-based online services or spend money on online gambling if they have access to means of payment. Some popular online role-playing games require a subscription and players can incur real costs for virtual goods or advanced virtual characters. Because of the lack of relevant data, it is hard to have a sense of the size of the problem.

Fraudulent transactions

Fraudulent transactions occur when children enter into a distance sales contract but, having paid, do not receive adequate value for money or find themselves tied into subscriptions. A notorious example from the mobile phone sector is the downloading of ringtones for mobile phones. Children may not realise that they pay additional costs or even that they have subscribed to a service for which fees are regularly debited to prepaid calling cards (YPRT, 2009, p. 12; Fielder *et al.*, 2007, p. 34). In 2008, 23.7% of Belgian teenagers reported having paid more for a ringtone than they expected and 7.5% had subscribed to such a service without realising it (Pouwels and Bauwens, 2008, cited in Hasebrink *et al.*, 2010, p. 154).

Economic risks are aggravated by children's inexperience, which renders them easy targets for online fraud and scams (YPRT, 2009, p. 12; ITU, 2009a, p. 33). Minors who do not yet have a bank account or credit card are less likely to incur immediate financial loss. However, they may still be victims of identity theft, and the exploitation of their personal data may result in false credit records (OSTWG, 2010, p. 16; Dooley *et al.*, 2009, p. 151).

Information privacy and security risks

Information privacy and security risks exist for all users. Children are a particularly vulnerable group of online users, however, because they often lack the awareness and the capacity to foresee possible consequences (*e.g.* disclosure of personal information online can potentially make it universally accessible) while existing safeguards may be insufficient to protect their online privacy and security effectively.

Children's information privacy

Children bear *information privacy risks* when their personal data are collected online automatically (*e.g.* cookies), upon request by an information service provider (*e.g.* when signing up for a service), or voluntarily, when they fill their personal information in online forms (YPRT, 2009, p. 11). Like most

adults, children tend to skip privacy statements of online services (Fielder *et al.*, 2007, p. 30; 30th International Conference of Data Protection and Privacy Commissioners, 2008) when they are written in a language too difficult for them to understand (Fielder *et al.*, 2007, p. 23; Dooley *et al.*, 2009, p. 146; Media Awareness Network, 2005, p. 17), and they readily agree to the use of their data in order to get access to desired websites. Services popular with children often fail to implement reliable procedures to ensure that parents are informed and give their consent on behalf of their children to sign in or create a user account online.[27]

Personal information as an online commodity

The fact that personal information is becoming an online commodity applies to children as well as adults. According to a 2007 study, 95% of British teenagers are concerned that personal information is being passed on to advertisers or other websites (Davies, 2007, cited by Byron, 2008, p. 157). Out of 40 favourite children's sites, almost two-thirds requested personal data, sometimes optionally, in order to access certain areas of a site: name (70%), e-mail address (53%), date of birth (43%), postcode (40%), address (24%) and mobile phone number (13%) (Fielder *et al.*, 2007, p. 25).

Some marketing targeting children through surveys, quizzes and contests, for example, collects personal information on children, their family and friends, often without regard to regulations requiring *informed parental consent.* The prospect of winning a prize or receiving a free service or a discount can be a compelling motivation to provide personal data (Dooley *et al.*, 2009, p. 145 f.). A report by the Australian Office of the Privacy Commissioner indicated that Australian youth are more likely to provide personal details to receive a reward or discount (the pull factor of prizes) (Dooley *et al.*, 2009, p. 145).

Because minors do not understand the business model of many Internet services, such as social network sites and online communities, they tend to underestimate the commercial interest of their personal data (YPRT, 2009; Fielder *et al.*, 2007, p. 38). Users are often not aware of the existence of a two-sided market, whereby online service providers offer services on the one hand and do business on the basis of users' personal information on the other. When children use such services, the challenge is to give adequate information about the purposes and extent of the use of personal data and to obtain parents' informed consent. Moreover, default settings rarely set the highest level of privacy protection for users known to be children. Finally, children and their parents can experience difficulties with complex privacy settings.

Children can be subject to *privacy-invasive practices* such as online monitoring, profiling (YPRT, 2009, p. 14) and behavioural targeting, without their knowledge and without knowing what precautions to take (UK Department for Children, Schools and Families, and Department for Culture, Media and Sport, 2009, p. 14, 84f.; Council of Europe, 2008c; Children's Online Privacy Working Group 2009, p. 8; OECD, 2010b, p. 7). Personalised advertising to minors also raises challenges regarding both exposure to commercial content (as noted earlier) and the sharing of children's personal data among service providers and within advertising networks. More generally, consumer groups warn about potential "negative impacts on children's future self-image and well-being" owing to the use of psychological, behavioural and social techniques in Internet advertising and marketing (TACD, 2009).

Sharing of personal data

It is important to take into account the context in which children voluntarily disclose information, which can range from disclosing personal data to the entire Internet to sharing personal information with friends. Recent research tends to find that children consider offline and online contexts as part of the same reality: they use the Internet primarily to socialise with people they already know and perceive the Internet as a private space for online social activities with peers. Moreover, children's attitudes towards privacy

differ not only according to age but also according to individual preferences which can be positively influenced by parental guidance (Marwick *et al.*, 2010, p. 13, 12).

Children may disclose personal data because they are unaware of the scope or breadth of the online audience and because they fail to take account properly of the potential consequences. For instance, minors have been early adopters of social networks, blogging platforms and other Web 2.0 applications, and they post information, images and videos that reveal a great deal of information about themselves, their family and friends. Children may presume, incorrectly, that all information they submit remains within the boundaries of their immediate contacts, and they may fail to anticipate the possible adverse consequences of providing information to "friends of friends", to people who may subsequently cease to be friends, and to those who may pass information on to others.

Children who are keen to create an online identity and to stay in touch with their peers are at risk of "oversharing", by divulging more and more personal information, including images. Peer pressure on social networks can perpetuate this tendency (Dooley *et al.*, 2009, p. 13, 143; Marwick *et al.*, 2010, p. 5, 20f.).

The extensive use of social networking websites by teenagers is well known. According to a 2007 Pew Internet Review, 51% of American teens had created a profile on a social networking website and 21% used it daily. Girls seem to be more active users of social networks (69% *versus* 50% of boys aged 15-17), and more likely to use them to communicate (32% *versus* 17%) and to post photos online (50% *versus* 37%). The use of social networking websites increases as children get older: 27% of 8-11 year-olds, 55% of 12-15 year-olds and 67% of 16-17 year-olds (Teens and Social Media, 2007, cited in ACMA, 2009a, p. 21). Similarly, in Australia, 51% of 8-11 year-olds use social networking services but 97% of 16-17 year-olds (ACMA, 2009b, p. 30).

Although young people feel strongly about privacy online, an increasing number of them reveal personal information. One study suggests that between 2000 and 2005, the percentage of young Americans who had shared personal data online increased from 11% to 35% (Wolak, 2006, cited in ISTTF, 2008, Appendix C, p. 40). This trend is likely to continue with the increased popularity of Web 2.0 applications where users post a great deal of personal data online. An American study (Pierce, 2007, cited in ISTTF, 2008, Appendix C, p. 40) found that 81% of young MySpace users posted their picture and 93% indicated their hometown. However, only 5% to 11% posted more sensitive information, such as their first and last names or phone number (Pew Internet & American Life Project, 2007; Pierce, 2007b, cited in ISTTF, 2008, Appendix C, p. 40). A recent Australian survey indicated that 74% of social network users revealed personal information such as e-mail address, name and date of birth (Model Criminal Law Officers' Committee, 2008, cited in Dooley *et al.*, 2009, p. 155). This may be a consequence of the rise of social networks such as Facebook, where real names and other personal information are given in order to connect with friends.

Moreover, although social networking sites such as Facebook, Bebo or MySpace have a minimum age of 13 for registering, an increasing number of younger children have created accounts. For example, in the United Kingdom in 2009, 22% of Internet users aged 8-11 said they had a social network profile, a 16% increase in 2008 (Ofcom, 2010, p. 5, 74). However, the number of young users making their profile public seems to decrease: 83% of 8-12 year-old Internet users said they were making their profile visible only to friends against 67% in 2008. Boys seem to be more likely (21%) to leave their profile open than girls (13%) (Ofcom, 2010, p. 74) but are also more likely (64%) to use fake data on their profiles than girls (50%) (Pew Internet & American Life Project, 2007, p.iii). Parents also seem aware that their child visits social networking sites, as 93% declared that they check what their child is doing on them.

Young people may not anticipate the long-term problems that may be created by the irretrievable, searchable, easy to manipulate and persistent nature of personal information online (YPRT, 2009, p. 11; Marwick *et al.*, 2010, p. 4). For example, there are many reports of young adults being rejected for jobs after their potential employers found text, pictures and videos revealing facets of their personality that they considered inappropriate.

Personal information can also be posted by someone else. For example *tagging* as a means of linking individuals to their digital photos, locations and events is now widely practiced and children do not, and do not need to, ask permission from the persons concerned (ENISA, 2007, p. 21; Grimm, *et al*., 2008, p. 11). While a study found that a little more than 40% of young people had had pictures of themselves posted online without their permission (Dooley *et al.*, 2009, p. 141), another one noted that 6% of youths reported having an embarrassing picture of themselves posted online without their permission (Lenhart, 2007, cited in ISTTF, 2008, Appendix C, p. 51).

Some studies note that young people consider sharing their passwords an easy way for their friends to check e-mail or social networking sites on their behalf, or as a mechanism to demonstrate trust (similar to knowing a locker combination) (Marwick *et al.*, 2010, p. 13). In 2003, 7% of Swedish children aged 9-16 said they had used someone else's e-mail or instant messaging without the account owner's permission. Similarly, 6% of Irish children admitted to having hacked into someone else's website (Hasebrink *et al.*, 2010, p. 154). In a 2008 study, among 13% of fourth through sixth graders and 15% of seventh through ninth graders in the state of New York, someone else had used their password without their permission. For a slightly smaller percentage, someone else had impersonated them online (McQuade and Sampat, 2008, cited in ISTTF, 2008, Appendix C, p. 42).

Minors' personal information, when spread online, can be linked to individual profiles and be used by third parties with malicious intent *(e.g.* in the context of identity theft). In 2006, the US Federal Trade Commission recorded 1 498 reports of identity theft from young individuals under 18 years of age, that is, 2% of all American identity thefts reported that year (Youn, 2008, cited in Dooley *et al.*, 2010, p. 155).

New possible threats for children's information privacy are the potential for abuse of *location-identifying information* from digital images (GPS data) and other location-based services (*e.g.* Loopt, Google Latitude, Facebook Places), which give clues about the whereabouts of a user (eNacso, 2009; YPRT, 2009, p. 30; De Haan and Livingstone, 2009, p. 11). In the case of mobile services, this can amount to real-time tracking of individuals if the service settings are not applied sensibly. In chats and other forums, the online status or availability of users is displayed and can be equally clear about their whereabouts.

The privacy protection paradox

Children have a need for privacy online as much as offline. They need, for example, to be able to socialise online with peers without constant supervision by parents and other guardians. There might be a "privacy protection paradox" if children are subject to "friendly" surveillance by adults as a way to protect them from offline and online risks, including privacy risks. For example, certain parental control technologies can provide detailed reports on online activities. Schools or libraries also increasingly monitor children's online behaviour as part of a cybersafety strategy (Marwick *et al.*, 2010, p. 15 f. and 61 f.).

Information security risks

Information security poses a challenge for Internet users in general; however, children are particularly vulnerable to information security risks stemming from *malicious code* (*e.g.* malware and spyware) (OSTWG, 2010, p. 16). They are unaware of the risks and use services with a higher risk of containing

malware. So far, there is only sporadic evidence of children being targeted as the weak link by online criminals, for example in order to infect the family computer which parents use for online banking.

Commercial spyware can be picked up on websites for children and stored on the user's device to monitor online behaviour (ITU, 2009a, p. 33; US FCC, 2009, para. 129). When the monitoring goes beyond what is necessary to perform the service, information may be collected from children for other purposes (*e.g.* online marketing). This use has been questioned in the context of children's information privacy (UK Department for Children, Schools and Families, and Department for Culture, Media and Sport, 2009, p. 51).

The heightened probability of information security risks is correlated with the popularity among young users of certain online activities which are conducted without appropriate safeguards. For instance, downloading files or opening e-mail attachments of dubious origin can plant malicious code on the user's computer. If not detected, it can damage the system or, more likely, steal sensitive information or take control of the computer and network as part of a broader cyberattack system (OECD, 2009b, p. 23). Although computers are the most common targets, malicious code exists for any electronic communications and online platform, including mobile devices (OECD, 2006, p. 39, 2009b, p. 23) and even social network sites (ENISA, 2007, p. 12), where profiles are hijacked in order to distribute spam.

While many children demonstrate advanced computing or digital literacy skills, a lack of risk awareness can explain negligence regarding information security. For example, the installation of file-sharing software and peer-to-peer programmes creates public access to the storage medium of the user's computer in order to facilitate the exchange, and can, if not properly set up, compromise personal files.

Lack of experience with assessing personalised messages critically and with noticing unusual circumstances can render children particularly vulnerable to *online scams*. Phishing attacks represent a common information security risk: users of all ages are lured to a website under a false pretext and enter personal or financial information (Dooley *et al.*, 2009, p. 149). Compromised information can be abused by identity thieves with various consequences even if it does not result in financial loss.

Conclusion

Risks vary from country to country depending on children's ability to access the Internet as well as on a range of social and cultural factors (Livingstone and Haddon, 2009, p. 17). For example the EU Kids Online research shows a positive correlation between use and risks when high-use countries are associated with relatively "higher risk" countries. Some countries do better than others: typically, research has found that in Denmark and Sweden high Internet use by children can be associated with medium online risks. This suggests a promising role for public policy (De Haan and Livingstone, 2009, p. 5; Livingstone and Haddon, 2009, p. 17).

As children's activities, skills and resilience vary, so do their interactions with the online environment and the related consequences. Children's vulnerability to online risks results from their lack of experience, awareness and critical capacity to fend off or manage risky situations. While these capabilities are likely to increase with age, so can their own risky behaviour.

The entire spectrum of risks can be observed in all countries, but prevalence rates vary and governments flag different issues as highly problematic. For example, online dating services and harmful advice in relation to suicide methods are at present of particular concern in Japan,[28] Finland sees online marketing and privacy issues as urgent for regulatory intervention,[29] and cyberbullying is highlighted as one of the most problematic areas in Australia, Canada and the United Kingdom.

The consequences of the risks vary and the most severe include physical and psychological harm. Economic impacts and long-term risks (*e.g.* enduring detrimental personal information online) should not however be underestimated. Information about the actual prevalence of risk and about factors that play a role in the materialisation of risks is essential in order to inform policy makers meaningfully (ISTTF, 2008, p. 13), and to avoid misrepresentation of risks and misguidance of public policy (Livingstone and Haddon, 2009, p. 22; Powell *et al.*, 2010, p. 6).

Recent reviews of empirical research on online risks for children in Australia, the European Union and the United States reaffirm the positive correlation between individual psycho-social and socioeconomic circumstances and risky behaviour (ISTTF, 2008, p. 5; Livingstone and Haddon, 2009, p. 16; OSTWG, 2010, p. 19; Dooley *et al.*, 2009, p. 165 f.). Other factors that influence the likelihood of encountering online risks include children's age and gender, which partly determine their online activities (Livingstone and Haddon, 2009, p. 16). This underlines the need for more research into these variables to identify more vulnerable groups and tailor risk mitigation strategies accordingly.

PART II: POLICY MEASURES TO PROTECT CHILDREN ONLINE

This section analyses existing policies to protect children online (for a more detailed overview, see Annex I), highlights commonalities and differences in approaches, and discusses possible means to reduce gaps and increase international co-operation.

Countries generally agree that the Internet offers a broad spectrum of opportunities for children in terms of their identity and self-expression, education and learning,[30] and, increasingly, their creativity, participation and online citizenship.[31] They also recognise that children's use of the Internet exposes them to various risks.

Countries therefore believe that children should be protected when they use the Internet and have taken various policy measures to mitigate their online risks. This section describes the three dimensions of policies for protecting children online and compares the main characteristics of different national policies.

The three dimensions of policies to protect children online

The various risks to which children are exposed online raise different policy issues, and most national policies to protect children online are complex: various policies tackle different risks and many initiatives from various stakeholders co-exist at different levels.

National policy measures reflect to some extent the classification of risks adopted in this report (see Part I), since they often address one of the three main categories of risks but rarely a combination of these. Conversely, when operators of websites adopt voluntary measures to protect child users from online risks, the approach is more inclusive and tends to reflect a wider spectrum of online risks for children.

The following discussion covers the various dimensions of child protection policy as they are implemented and pursued in most countries: *i)* multi-layered policies comprising direct and indirect policy tools; *ii)* multi-stakeholder policies related to the various roles and responsibilities of stakeholders; and *iii)* multi-level policy mechanisms at national and international levels.

Multi-layered policies

The protection of children online is a relatively recent area of public policy concern, and many countries are in the process of re-assessing existing policies and formulating new policy responses. Some countries are more advanced than others in this area.

Countries such as Australia, Canada, and the United Kingdom have devised national strategies which pull together various instruments and activities at policy and operational levels. In Australia and the United Kingdom, the visibility and transparency of their national policies to protect children online has promoted an overall understanding of policy makers' key challenges. Countries such as Japan and the United States have partial strategies and measures to protect children online; policies implemented by various agencies and ministries are not necessarily part of a single strategic vision. Both national and partial strategies can help make the Internet a safer place for children. The EU Safer Internet Programme (SIP) provides an

example of a regional effort that plays a key role in promoting child online safety across a large group of countries.

All countries' approaches blend legislative, self- and co-regulatory, technical, awareness, and educational measures, as well as positive content provision and child safety zones. However, the degree to which countries rely on each of these policy tools varies. It is not at present possible to compare the effectiveness of high-level policies owing to a lack of comparable evidence to make a case for best practices.

Legal measures

Most countries would subscribe to the statement that what is illegal offline should be illegal online and champion a normative approach to child protection online. In such countries, the main challenge is to enhance the compliance with and enforcement of existing instruments rather than adopt additional laws and regulations.

In a majority of countries, regulation of online content is a cornerstone of their national policy framework. It generally applies to content published on the Internet rather than to content passed on via individual data exchange. Content regulation takes a two-pronged approach: a general ban on illegal content and national regulation of child-inappropriate content up to defined age levels (Australia, Korea, Japan, New Zealand and most European countries). The definitions of illegal and child-inappropriate content are subject to national interpretation and reflect cultural and societal values. Most countries have updated content regulations to include the Internet (*i.e.* horizontal regulation), some have passed Internet-specific legislation (Japan, Korea, Turkey) and a few (Canada and the United States) have by and large refrained from issuing new legislation, not least because of constitutional requirements. However, to some degree the normative substance cascades to soft law and can be revisited in self- and co-regulatory schemes.

Contact-related risks, in which children are harmed by others, are punishable as a criminal offence in some countries. Cybergrooming is a new type of criminal offence and is codified by several countries.[32] As necessary, countries update their criminal code to capture that a criminal offence is committed via electronic communications (*e.g.* harassment is extended to include cyber-harassment). Cyberbullying is a borderline case. Depending on its severity, it may be punishable under existing harassment laws. Often, however, when the aggressors are children, a different policy approach is needed.

The protection of children against consumer-related online risks is to some extent addressed through legal measures related to regulated activities. For example, in many countries online gambling cannot be offered to minors. For online marketing targeting children, countries either tend to regulate certain aspects (in the EU only the Scandinavian countries have comprehensive regulation) or promote self- and co-regulation (Australia, Canada and the United States).

There is no specific legislation to mitigate information security risks for children.

Countries report unanimously that legal safeguards are under considerable strain for reasons that are inherent to the Internet as a global and highly dynamic information space. A number of countries recognise that the Internet has outpaced legal definitions and normative concepts and that legal patch-ups can quickly become outdated if they focus too narrowly on a specific use or technology. Consequently, some countries have embarked on flexible, technology-neutral policies where appropriate, such as the regulation of child-inappropriate content in all media, regardless of the mode of delivery.

A number of countries have moved towards regulating or otherwise committing Internet intermediaries to comply with so-called "notice and take down procedures" (mandatory in Australia, Italy, Japan, Korea and Turkey) or to introduce mandatory filtering schemes (Turkey, planned in Australia).

The efficiency of legislative frameworks for protecting children's privacy ought to be examined as no law is self-enforcing. In most jurisdictions (*e.g.* Canada, European countries) general data protection laws apply to the collection of children's personal data; there are no specific provisions.[33] However, the United States provides an example of a targeted legislative response, the Children's Online Privacy Protection Act (COPPA),[34] which protects children up to the age of 13 and requires website operators targeting these children or having actual knowledge of child users to collect verifiable parental consent. Under COPPA, the age up to which legal protection is afforded is clear although this threshold age is one that is often discussed in the child advocacy community as to whether it is appropriate. Japan has specific guidelines for students' data protection at school, "Guidelines concerning the measures to be taken by entities to ensure the proper handling of personal information of students and others at schools", which is mainly applied for enforcing of the Act on the Protection of Personal Information to private schools handling students' personal data. It concerns the rights of students, and has clauses concerning the danger of child abuse and domestic violence when statutory agents of children (parents in many cases) demand the disclosure of retained personal data of children.[35]

More specifically, limits to the consent requirement, discussed elsewhere by the OECD (2010a), are aggravated by the lack of effective mechanisms for obtaining parental consent. Other protections required by privacy laws, whether online or offline, such as privacy notices or the right of access, are unlikely to be more effective for children and their parents than overall. Moreover, in the online context the data controller cannot easily verify the age of the data subject.[36] While specific protection measures are probably less difficult to implement for online applications that obviously target children, applications that target the whole population do not have an easy and efficient way to distinguish children from other users.

As ever younger children increasingly use the Internet, the actual level of protection afforded by current legal data protection mechanisms with respect to the collection of their personal data is low.

The complexity of laws and regulations pertaining to the Internet, and more specifically aimed to make the Internet a safer place for children, should not mask the fact that legal measures alone are insufficient to achieve this goal. Combinations of complementary policy measures, such as legally twinning prohibitions with technical access restrictions to child-inappropriate content (*e.g.* Germany), are an attempt to make online content regulation more effective.

Self- and co-regulation

Governments tend to agree that self- and co-regulation can be expedient. Voluntary commitments can be better tailored to specific situations (*e.g.* social networking sites) and updated in order to stay abreast with technological developments and social trends which are the particular strengths of this model (IT, 2009a, p. 5; ITU, 2009b). Self- and co-regulation approaches have to stay consistent with overall fundamental rights and communication freedoms.

Self- and co-regulation are ways for industry to support efforts to protect children online. For example, Internet intermediaries voluntarily commit to give effect to national policies by adhering to notice and take-down regimes and/or voluntary filtering of certain types of illegal content. High traffic websites such as social networking services can promote better cyber-safety practices and standards, in particular where governments have no jurisdiction. When markets are concentrated as a result of substantial network effects – social networks, online communities, search engines – the largest providers are also best placed to protect the children among their users. Many countries therefore promote self- and co-regulation, for

example through public-private partnerships, as evidenced by the many voluntary commitments of Internet service providers and their national associations, on the one hand, and of social network site operators in the EU and the United States, on the other.[37]

Consolidation of existing self- and co-regulation to protect children online, common framework principles across industries, and independent evaluations would make this model even more effective (Byron, 2008, p. 180; Livingstone and Haddon, 2009, p. 26; ITU, 2009b). For example, governments promote sectoral and, where appropriate, cross-sectoral consolidation of voluntary codes for the protection of children online (*e.g.* the notion of a child in the context of online marketing) as well as improved accountability mechanisms. Government collaboration with other intermediaries, such as online advertising networks, can provide another avenue for protecting children against inappropriate marketing.

Technical measures

Governments also understand that there is no "silver bullet" solution and that each technology has its strengths and limitations and should be used in the most appropriate context. Recent reviews of the most advanced technology to protect children online find significant progress, which yields “cautious optimism” (ISTTF, 2008, p. 5). Some technology-driven mechanisms, such as report abuse functions and content labelling frameworks, demonstrate the usefulness of technical measures to mitigate risks and enhance online safety for children. Apart from improving the performance, reliability and usability of technology, future efforts should strive to improve interoperability across a wider variety of distribution platforms and devices (ISTTF, 2008, p. 28; US FCC, 2009, para. 175).

National policies vary greatly in their reliance on technical measures. Countries such as Australia and Japan have spearheaded the adoption of technical safeguards. Overall, however, there is no overreliance on technology. Governments generally promote and sometimes mandate technical measures at various levels in concert with other risk-mitigation strategies. For example, technical measures often complement legal obligations, as when national content regulations require that child-inappropriate online content be subject to access controls, *e.g.* age verification systems.

Essentially, when countries resort to mandatory filtering of the Internet, the measures necessarily apply to the whole population and are therefore used - if at all - to suppress illegal or criminal online content. For example, the dissemination of images of sexual abuse of children is subject to filtering obligations in some countries (*e.g.* Italy; in Germany it is a legal obligation but it is not implemented) and the European Union and other countries are exploring this policy option in the interest of victims. There are concerns that the gradual expansion of mandatory filtering to other topics might affect freedom of expression.

In a range of countries, filtering schemes operate as part of the voluntary commitment of Internet service providers to block access to illegal content and in particular to images of sexual abuse of children.

Outright prohibitions and mandatory filtering at the level of Internet service providers (ISPs) are generally not used for content that is child-inappropriate or harmful to minors, as this would make the Internet a child-safe zone for all users.

Public policy can promote voluntary technical options such as parental controls by enhancing awareness of their availability and confidence in them (*e.g.* the UK Kitemark label[38]). Apart from illegal content, voluntary technical solutions are flexible and can be customised. No countries so far require or encourage, as a general policy, software settings to be preset to protect children online (*i.e.* child protection by default) except when users are known to be children. Future efforts should concentrate on making it

easier for users, and parents in particular, to manage technologies and personal settings to protect children.[39]

Besides devices designed and configured for children and the possibility to bar or restrict certain functionalities, for example of mobile phones, for child users, software design plays an important role in protecting children online. Private companies that collect a great deal of information about children need to emphasise software design that makes privacy settings and rules easier to adjust and to understand for children and their parents (Marwick *et al.*, 2010, p. 66 f.).

Awareness raising and education

Awareness raising and education seem to be recognised across countries as important policy tools that help to empower children, parents, caregivers, guardians and educators. Effective and sustainable awareness campaigns refrain from fearful messages (ITU 2009a, p. 5; Marwick *et al.*, 2010, p. 262), address opportunities and risks together, and promote active risk mitigation and coping strategies (Livingstone and Haddon, 2009, p. 23).

The current trend to integrate media and/or Internet literacy in school curricula can be an effective way to equip children with the knowledge and skills necessary to stay safe online and use the Internet to their benefit. The content and learning outcomes of Internet literacy courses vary widely, with many countries emphasising cybersecurity (*e.g.* United States) and information ethics (*e.g.* Japan).

Given that policy can mitigate but not totally eliminate all online risks, Australia, New Zealand and the United Kingdom have embarked on a more inclusive concept of Internet literacy. The notion of digital citizenship education carries Internet literacy forward to include coping strategies, and trains children to engage responsibly in creative and participatory online activities (ACMA, 2009a, p. 50; Livingstone and Haddon, 2009, p. 25; YPRT, 2009, p. 32 f.; OSTWG, 2010, p. 5).

Where the aggressors are often children themselves (*e.g.* cyberbullying) preventive policy approaches are particularly relevant, such as prevention and intervention in schools, training in coping behaviour and awareness raising on the part of parents and other caregivers.

Positive content provision and child safety zones

EU members and some other countries believe that protecting children online also involves creating a positive online experience. In some countries, this entails the provision of positive online content for children, sometimes publicly funded and/or carried out under the remit of public service media (*e.g.* in many European countries). Germany for instance is supporting the creation of high-quality and innovative Internet content for children with an annual budget of EUR 1.5 million over a three-year period. The provision of positive online content for children can be challenging as it must stand comparison with other Internet services.

Not all content targeting children can be considered positive online content for children, as the determination of such content is in most cases left to the provider. Conversely, portals that restrict access to approved services ("walled gardens") generally maintain a definition of content which is suitable and therefore admissible within their service. Such safe online zones can be a solution for younger children, but innovative approaches are needed to stimulate the production of a wider array of suitable content. Experiences such as Kids.us or the Belgium Saferchat initiative have shown that the main source of failure is the lack of attraction for content producers and/or children.

Multi-stakeholder effort

There is a common understanding that an online child protection policy rests on the commitment and shared responsibilities of all stakeholders. It is therefore essential to identify participants and define their role.

Governments and public authorities

The adoption of clear policy objectives at the highest government level provides leadership and gives higher visibility to national policies to protect children online. It helps to engage all stakeholders and to facilitate co-ordination of efforts. Many governments have taken up online child protection at the cabinet (*e.g.* Australia, Japan) or ministerial (*e.g.* the United Kingdom) level.

Some countries have created new bodies to co-ordinate the activities of public and private stakeholders, such as the United Kingdom Council for Child Internet Safety, or to inform government policy and advise on research projects, such as the Australian Consultative Working Group on Cybersafety.

Some countries have set up new bodies, such as the children's rights ombudsman in Poland or the Hungarian Ombudsman for Future Generations, which can supplement but not replace high-level government involvement. Other authorities involved include law enforcement, media regulators and classification bodies, specialised public agencies (*e.g.* the Turkish Internet Regulations Department), communications regulators (*e.g.* the converged United Kingdom regulator Ofcom), data protection authorities (*e.g.* Office of the Privacy Commissioner of Canada) and various governmental departments concerned with culture, education, youth and family.

A concerted policy approach requires clear responsibilities and co-ordination among all public bodies involved.

Children

Children have a right to freedom of expression and of communication as laid down in Article 13 of the UN Convention on the Rights of the Child and in countries' constitutions. It is also widely recognised that children differ in age, degree of vulnerability and/or resilience, and that some are more at risk than others. Therefore, it is commonly understood that policies to protect children online must be tailored to their needs, risks and stages of development.

In many countries certain educational approaches are adapted to specific age groups and policy makers emphasise that filters such as those deployed in parental controls should therefore be customisable. There are certainly limits to the granularity and individuality that public policy can accommodate. Besides integrating Internet literacy in schools' curricula, little or no information is available on effective strategies for identifying and reaching out to categories of children who are more at risk than others, such as those whose parents cannot play the role expected of them in a policy model based on shared responsibility.

The EU and some individual countries (*e.g.* Australia, United Kingdom) recognise children as active stakeholders in their formulation of policy and implementation processes (ACMA, 2009, p. 25). Children are invited to participate in forums at which they can give their views on online risks and policy measures.[40] Involving children more actively in developing such policies can contribute to better policy measures. Children can also be more engaged in peer education strategies and can help relay information about online risks and risk mitigation strategies.[41]

Parents and caregivers

All countries' policies rest to varying degrees on voluntary measures taken by parents and other caregivers to protect children online. All countries acknowledge that parents have a special role and responsibility in the education of their child. Where government intervention in Internet content control and online activities is minimal (*e.g.* Canada, the United States), the role of parents is even more central. Parents have various means to assist their child and mitigate online risks, such as parental guidance and rules on when and how to use the Internet as well as technical tools such as parental control software.

However, to act effectively, parents must be provided with information and appropriate tools, and even then, there are limits to what they can and will shoulder.[42] Some countries have started to gear many policy measures towards parents, with a focus on awareness raising, child safe zones and online positive content provision, and the promotion of parental controls. For example, the United Kingdom Kitemark scheme not only considers whether a technology is efficient but also whether it is easy to install and to set up for parents. Given the numerous entry points for parents willing to protect their children online, countries could consider consolidating advice and promoting parental control solutions which work across various platforms and technologies.

Educators and public institutions

The role of educators, social workers and other trainers in children's Internet literacy is generally acknowledged, as is the need to protect children when they use online facilities of public institutions such as schools and libraries.

Some countries have introduced Internet safety training for educators and started to include Internet literacy training in teachers' education (*e.g.* Australia, United Kingdom). In most countries, approved awareness materials and teaching resources are made available to educators (*e.g.* Australia, New Zealand) and can be used with students. The training of teachers and their access to suitable teaching resources is essential for a successful Internet literacy strategy.

Public institutions are often required by law, encouraged or given incentives to adopt technical measures and institutional policies in order to protect children. For example, in the United States, funding of public institutions is tied to the adoption of policies (*e.g.* anti-harassment policies, acceptable use policies) and technical measures (*e.g.* filters) to help protect children and enhance responsible use of the Internet.

Private sector

The key role played by private-sector actors to protect children online is broadly recognised. Many service providers have accepted responsibility for introducing more nuanced safeguards for children and for self-policing their websites and implementing use policies. Many countries actively promote industry self- and co-regulation in order to implicate the private sector and enhance compliance.

Many non-profit private organisations work to make the Internet a safer place for children. In some countries these organisations have been instrumental in national multi-stakeholder collaboration. In many European countries national awareness centres have become significant national policy platforms.

Multi-level policies

At the national and international level, online child protection policies aim to achieve policy and operational collaboration.

National level

Many governments recognise their mandate to protect children online and understand that national efforts must be in the child's best interests, in line with Article 3 of the UN Convention on the Rights of the Child. As this is the aim of a variety of public policy measures and private initiatives, the role of public leadership extends beyond "command and control" intervention to co-operation, co-ordination, assistance and support to stakeholders. Often, government efforts help steer problematic issues with other stakeholders.

Given the complexities of policy making in the area of protecting children online, some countries have opted for a more holistic policy framework in which national priorities are defined with a view to enhancing policy coherence (*e.g.* the EU within its competences, Australia, Canada and the United Kingdom). Australia's 2008 Cybersafety Plan is a good example of national strategy. It has committed some EUR 81 million over four years, among others to cyber-safety education and awareness-raising activities, law enforcement, and the exploration of a national content filtering scheme expected to become mandatory for Internet service providers.

In general, governments already have in place some child protection legislation and other measures. Stocktaking exercises to provide an overview of the various public and private initiatives that protect children online might be useful to inform policy makers. Mapping the various initiatives and stakeholders would also highlight interdependencies, interfaces and feedback mechanisms.

Policy development, co-ordination and management need to be sufficiently resourced, including in countries that rely heavily on market mechanisms and parental responsibility. To this end, some governments provide the infrastructure and secretariat for a national steering committee (*e.g.* the United Kingdom) or fund non-profit organisations (*e.g.* New Zealand). Better co-ordination can improve policy performance and create efficiencies which outweigh the initial investment.

International co-operation

Countries generally consider international co-operation essential for protecting children on an inherently global medium. Beyond sharing best practices, international co-operation at the operational level has produced a number of promising initiatives which can serve as models.

International co-operation at policy level

As fits their mandate, membership and areas of expertise, various international bodies are involved in an international dialogue on the protection of children online, *e.g.* the ITU's Child Online Protection (COP) Initiative and the Dynamic Coalition for Child Online Safety in the framework of the Internet Governance Forum (IGF). Policy frameworks such as that of the Council of Europe on the protection of minors against harmful content and on developing children's media literacy skills have achieved a high degree of policy co-ordination at regional level. Table 2 summarises the main initiatives of international organisations and advances in cross-border co-operation towards the protection of children on the Internet.

Table 2. Initiatives for international co-operation by intergovernmental organisations

Organisation	International co-operation activities
APEC	• On 15 April 2009, APEC and the OECD held a joint symposium to exchange best practices on the protection of children online (APEC TEL 39, Singapore). • In May 2010, APEC launched a project to build the capacity of APEC law enforcement agencies to respond effectively and offer greater protection to children from cyber-safety threats (APEC TEL 41, Chinese Taipei).
Council of Europe	The Council of Europe addresses cybercrime and the sexual exploitation and abuse of children through information and communication technologies by: • Setting common standards and policies, *i.e.* introducing criminal offences against online images of sexual abuse of children and against sexual solicitation. • Preparing a global study (ongoing) on Criminal Law Measures to Protect Children Against Sexual Exploitation and Abuse. • Conducting a Europe-wide campaign against sexual violence against children with particular reference to new media (planned for autumn 2010). • Providing own resources for educative and preventive measures and to empower children.[1]

ITU	ITU pursues its work on Child Online Protection at policy and operational level:
	• Child Online Protection (COP) Initiative is a multi-stakeholder effort of ITU membership to create awareness and to develop practical tools and resources to help mitigate risks.[2]
	• Council Working Group on Child Online Protection[3] (CWG-CP) is a platform for member states, sector members and external experts to exchange views and advance the work on child online protection, in particular by:
	  ○ developing reports on the source of online threats to youth and children and on social networking services and policies with regard to user-created content;
	  ○ devising ITU's Child Online Protection Statistical Framework and Indicators (ITU, 2010b).
	• On the 2009 World Telecommunication and Information Society Day (WTISD) ITU announced a year-long call for action on child online protection.

OECD	• At the Seoul Ministerial Meeting on the Future of the Internet Economy (June 2008), Ministers encouraged collaboration between governments, the private sector, civil society and the Internet technical community to build understanding of the impact of the Internet on minors in order to enhance their protection and support when using the Internet. They declared that they will increase cross-border co-operation of government and enforcement authorities in the area of protecting minors. • In April 2009, the OECD held a joint workshop with APEC in Singapore (see above). • In 2009, the OECD Working Party on Information Security and Privacy launched a project to analyse risks faced by children online and policies to protect them and, as appropriate, develop policy guidance/principles in this area.
UNICEF	UNICEF focuses on the protection of children from violence, exploitation and abuse. The UNICEF Innocenti Research Centre is currently preparing a study on sexual abuse and exploitation in the converged online/offline environments.
WSIS/ IGF	The outcome documents of the World Summit on the Information Society (WSIS) contain strong commitments on the protection of children online: • The Geneva Declaration of Principles states that the development of ICT applications and operation of services respects the rights of children as well as their protection and well-being. • Paragraph 24 of the Tunis Commitment recognises "the role of ICTs in the protection of children and in enhancing the development of children". The commitment calls to "strengthen action to protect children from abuse and defend their rights in the context of ICTs", emphasising "that the best interests of the child are a primary consideration". Its successor, the Internet Governance Forum (IGF), provides an annual international and multi-stakeholder platform to exchange views on children and young people, among others.

1. *www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Protecting%20children/Default_en.asp*

2. *www.itu.int/osg/csd/cybersecurity/gca/cop/*

3. *www.itu.int/council/groups/wg-cop/*

International co-operation at operational level

Several successful international co-operation initiatives at operational level have already been carried out, in the areas of law enforcement, exchange of hotline reports about illegal online material (*i.e.* INHOPE) and sharing of best practices for the protection of children online (*i.e.* INSAFE). The networking of hotlines and awareness centres is a successful initiative which could be strengthened and further resourced. These networks could also inspire similar initiatives with different goals.

The development of comparable indicators to measure various aspects of the protection of children online, from access and use of the Internet by children to risk prevalence and the impact of policies could help improve policy development and implementation. EU efforts in this area have helped, for example, to better understand the relationship between Internet use and online risks and the positive role public policy can play in the mitigation of online risks. As can be seen from the EU Kids Online project, countries benefit greatly from the availability of evidence reviews, up-to-date surveys and comparative data.[43]

Awareness raising is another area in which international co-operation can be beneficial. Simple measures such as the use of light intellectual property protection on educational materials can be of great interest to other countries, who could tailor them to their national context. Hector's World for example was developed with a view to being made available internationally.[44] The Safer Internet Day has proven international appeal and could be supported by more organisations and in more countries.

Enhanced interoperability of technical measures such as parental controls across distribution platforms and devices (ISTTF, 2008, p. 20) requires international co-operation for setting standards. The Quarto+ project, for instance, develops an inclusive and open international standard for interfaces between content classifications and filtering technologies which does not require harmonisation of national content rules.

Comparative policy analysis

It is commonly agreed that the main challenge for protecting children online is to combine the available direct and indirect policy measures described above. In practice, countries operate a national policy mix with varying characteristics and priorities which correspond to their legal system and governmental culture.

Parallels in countries' high-level policies

Awareness raising and education are generally recognised as key policy tools, albeit with varying scope and intensity. Besides these two important dimensions, countries can be divided into three groups reflecting how they address other policy tools: *i)* those in which a combination of legal and technological measures prevails; *ii)* those that favour self- and co-regulation and voluntary measures; *iii)* those in which no type of measure predominates in the policy mix.

Australia, Japan, Korea and Turkey generally belong to the first group which emphasises the combination of legal and technological measures, including the voluntary introduction of technical safeguards. These countries updated their legislation (*e.g.* Australian Broadcasting Service Act) or introduced new Internet-specific legislation (Japan, Korea and Turkey). They maintain content regulation to address content that is illegal or harmful to minors (the classification can have further granularity) and they encourage or require mandatory filtering of illegal content by ISPs. In addition, service providers are sometimes required to deploy technical measures that help protect children, such as filters on mobile phones of under-age users in Japan or the use of approved filter services in cybercafés in Turkey. There also tends to be a strong self- and co-regulatory component with regard to content- and contact-related risks and public encouragement to install voluntary technical safeguards such as parental controls.

Canada and the United States are representative of the second group of countries. They pursue a "soft law" approach by promoting self- and co-regulation and voluntary measures, including the voluntary use of parental controls. Both emphasise education and awareness raising. Self- and co-regulation by popular social network and community sites are a source of normative content provisions and voluntary agreements to improve protection of child users and self-police their services. The body of self- and co-regulation in these countries appears to be very diverse, with little consolidation across industries and service clusters.

Finally, the EU and European countries tend to make use of all policy measures with combinations varying according to risk categories. These countries commonly adopt legislation related to content-related risks and oblige service providers to prevent children from accessing inappropriate content. Consumer-related risks for children online are partially regulated and partially subject to self- and co-regulation. Typically, the introduction of technical filters and other safeguards by industry is based on voluntary commitments by ISPs and other Internet intermediaries and are often the result of co-regulation or brokered in public-private partnerships. Educational and awareness-raising measures form an integral part of national policy, with variations from north to south and east to west.

Countries not included in one of the three groups are not inactive but do not pursue a clear policy towards protecting children as Internet users against online risks and may have different pressing policy priorities, such as combating online forms of sexual abuse and exploitation of children, as in Thailand and the Philippines.

Definition of a child

Within a given country, there is often a lack of consistency regarding the age thresholds up to which children are protected both within a single risk category and across the spectrum of online risks. Age thresholds are often the result of the legacy of existing legal instruments and self- and co-regulatory mechanisms. They are rarely reconsidered with a view to increasing harmonisation within and across risk categories. When this lack of consistency is not justified by sound analysis of the risk context, it makes the overall child protection policies more complex and may reduce their effectiveness. Governments and stakeholders could work together to consolidate the age up to which children should be protected and agree on generic age cohorts (*e.g.* small children, children, adolescents) spanning at least one risk category and, wherever possible, across various risk categories.

As noted earlier, the lack of harmonisation of age cohorts is also a serious obstacle to international comparisons of the prevalence of risk and of policy efficiency. A common definition of children's age cohorts across countries and among stakeholders would help establish standards at the regional and international levels. More consistent age limits would also facilitate the implementation of protection mechanisms for online services providers operating in several countries.

Combinations of policy measures

An analysis of existing policies to protect children online (US FCC, 2009, p. 61; EC, 2008b, p. 27) reveals that no country relies solely on one policy instrument to tackle a risk category. Policy measures are combined to reinforce each other (*e.g.* promotion of parental controls and awareness raising among parents about their availability). Generally, countries consider that education and awareness raising are very important complements to online child protection policy.

Combinations of complementary policy measures pertaining to certain risks, such as normative and technical measures (*e.g.* online gambling prohibitions for children and mandatory age verification systems for online gambling websites in the United Kingdom) are clearly emerging. The implementation of "effective access restrictions" is often mandatory for certain websites, but the choice of appropriate

measures it is left to the market. Even more complex combinations of policy instruments are emerging, notably when regulation of online content is implemented through labelling and classification schemes combined with various modalities of access restrictions on the part of website operators and the voluntary use of parental control technology.

Table 3. Examples of complementary policy measures mandated by law

Country	Policy measure	Complementary technical policy measure
Korea	Regulation of child-inappropriate content	Access restriction via reliance on national identity verification systems
Italy, Korea, Turkey	Regulation of prohibited and illegal content	Mandatory ISP-level filtering
United Kingdom	Online gambling prohibition	Online gambling websites are required to put age verification in place
Japan	Regulation of child-inappropriate content	Mandatory filters on mobile phones of users under 18 unless parents opt out
United States	Parental consent requirement under COPPA	E-mail from parents' e-mail account, provision of parents' credit card details, written consent form from the parent, or telephone call from parent.

Use of evidence, policy assessments and performance evaluations

To inform and evaluate public policy to protect children online, some countries increasingly seek information and evidence on the availability, feasibility and – to a lesser extent – effectiveness of measures. Many countries have started to build a knowledge base:

- Expert reports and original research are contributing significantly to understanding how children use the Internet and how they are affected by the Internet as well as the prevalence of risk.[45]

- Feasibility and technical studies provide insight into how technical measures can help mitigate online risks for children and into the development, reliability and shortcomings of technologies.[46]

- Public consultations are used in the review of policies and to collect stakeholders' input.[47]

- With some notable exceptions, the impact of regional and national policy frameworks for child protection online is not regularly assessed, and performance evaluations are only exceptionally built into the policy, notably when third-party measures are publicly funded. The lack of assessment of the policy impacts of certain measures, notably on freedom of speech and privacy, can be observed at all levels and raises concerns among all categories of stakeholders. Most voluntary commitments to protect children online foresee no regular mechanism for demonstrating their effectiveness. This hampers the transparency and accountability of voluntary schemes. Likewise, awareness raising and Internet literacy, which are at the core of many national policies, would benefit from better monitoring of their effectiveness.

Exceptions include the EU's Safer Internet Programme, which incorporates a social and economic impact assessment of policy formulation and independent evaluations of the measures adopted,[48] and the UK Child Internet Safety Strategy, for which progress will be evaluated on the basis of pre-defined targets and benchmarks.[49]

Examples of the evaluation of voluntary commitments include the European Framework for Safer Mobile Use by Younger Teenagers and Children and the Safer Social Network Principles (PricewaterhouseCoopers, 2009; Staksrud and Lobe, 2010).

Finally, awareness raising and education programmes are rarely evaluated or assessed (OSTWG, 2010, p. 6; Powell *et al.*, 2010, p. 12). Examples of independent evaluation include the United Kingdom's Ofcom-funded evaluation of the delivery of the Know IT All presentation (Woollard *et al.*, 2007) and a study assessing the effectiveness of the NetSmartz programme (Branch Associates, 2002).

While many countries are building up a knowledge base (ACMA, 2009, p. 18 f.), very few (Australia, the United Kingdom and to some extent the United States) have started to link research with policy formulation and policy assessment. Most countries do not systematically use evaluation tools such as impact assessment and performance evaluation. They thus forego the opportunity to learn systematically about achievements, failures and the need for adjustments.

PART III: KEY FINDINGS

The protection of children against risks online is an emerging policy area which raises complex and evolving challenges. The preceding overview of existing policies shows that this is a relatively new policy area when compared to more traditional Internet issues, but that a variety of policy tools are available. It also shows that most government policies:

- Are based on the common understanding that:
  - the protection of children online requires a careful balance between the risks and opportunities presented by the Internet;
  - the dynamic and universally accessible nature of Internet content challenges national policies;
  - this policy issue calls for a combination of public and private, legal and voluntary measures at various levels;
  - all stakeholders share responsibility for protecting children online and co-ordination of their roles is necessary;
  - international co-operation at policy and operational levels is essential to protect children online successfully and to mitigate risk (Muir, 2005, p. 6).
- Are complex because they combine:
  - multi-layered measures – legal, self- and co-regulatory, technical, educational as well as awareness raising;
  - multi-stakeholder initiatives that involve government and public authorities, children, parents and caregivers, educators and public institutions, and the private sector;
  - multi-level approaches at national and international levels, at policy and operational levels.

Several national and international bodies have issued recommendations on policies for the protection of children online, including the US Internet Safety Technical Task Force (ISTTF) and Online Safety and Technology Working Group (OSTWG), the reports of the Australian Communications and Media Authority (ACMA), the EU Kids Online project, the European Youth Protection Roundtable (YPRT) and the International Telecommunications Union (ITU) Guidelines for Policy Makers of Child Online Protection (2009a). Building on these recommendations and on the comparative analysis of the policies provided in this report, this section presents key policy findings for the consideration of policy makers.

Policy coherence

Governments all aim for multidimensional policy making that does not compromise efficiency. However, ensuring the co-ordination and consistency of policies to protect children online and their alignment with sectoral policies such as information society policies is a challenge. The policy coherence framework (see Box 1) can encompass government policies, including measures that encourage non-governmental actions, notably initiatives by business (*e.g.* through self- and co-regulation and other voluntary commitments) and other stakeholders.

Box 1. The dimensions of policy coherence

Coherence has a number of dimensions which need to be addressed together, although it must be recognised that it is not realistic to expect full coherence.

- Policy ***co-ordination*** means getting the various institutional and managerial systems that formulate policy to work together.
- Policy ***consistency*** means ensuring that individual policies are not internally contradictory and avoiding policies that conflict with reaching a given policy objective.
- Policy ***coherence*** involves the systematic promotion of mutually reinforcing policy actions across government departments and agencies with the view to achieving a defined objective.

Source: OECD (2001, p. 104; 2003, p. 2).

Co-ordination

The aim of policy co-ordination is to combine the institutional and managerial processes and tools at governments' disposal to devise, influence and promote a variety of policy measures which operate together so that children are protected effectively online. Public-private partnerships have proven a successful organisational model to catalyse effective self- and co-regulation. This model could be taken further.

Effective co-ordination entails examining how different policy measures interact, whether interdependent measures work well together, and how to optimise interfaces among the various policy measures. Means to this end include steering committees, either government-led or in which government participates with all stakeholders, which examine various feedback mechanisms, define national agendas and evaluate and adjust national policies where necessary. The United Kingdom provides an interesting example in the Council for Child Internet Safety, an organisation composed of 150 stakeholders and tasked with developing and implementing a Child Internet Safety Strategy.[50]

Switching from an aggregation of fragmented public and private policy initiatives to a strategic vision with high-level leadership and long-term commitment helps increase the efficiency of existing and future policy efforts. Good co-ordination also leads to cost savings and can translate into cost efficiencies.

Consistency

Policy consistency aims to ensure that individual policies are not internally contradictory and do not conflict with the realisation of a given policy objective. It can be achieved by reducing inconsistencies

(*e.g.* definition of a child) and by consolidating public information and guidance (*e.g.* use of harmonised expressions such as "parental controls"). Consolidation has also been identified as an important means to simplify the protection afforded by self- and co-regulation and private policies.

The interdependence of online opportunities and risks for children draws attention to the need for consistency, as some strategies designed to protect children online may reduce the benefits they can obtain from the Internet. Developing measures that prevent and mitigate risks without unduly reducing the benefits of the Internet for children requires a thorough understanding of the relationship between risk incidence and/or harm, the prevalence of online risks, and the impact of policy measures (Powell *et al.*, 2010, p. 6). Public policy has to be flexible to accommodate the various development stages and vulnerabilities of children.

Another important policy objective is to remain consistent with fundamental rights and values. These include the right of children - as for other Internet users - to freely receive and impart information (*i.e.* freedom of expression) (UN Convention on the Rights of the Child, Art. 13). They also include the right to privacy (UN Convention on the Rights of the Child, Art. 16). This is a particularly acute issue as regards technical measures to protect children online which affect all Internet users. Similarly, policy measures to protect children online should not unsettle the framework conditions that have enabled the Internet to become an open global platform for innovation, economic growth and social progress (OECD, 2008, p. 17). Voluntary commitments and self- and co-regulation should also respect these boundaries. Government policies which rely on voluntary commitments by Internet intermediaries should ensure that appropriate safeguards are in place.

The technical aspects of child protection policy online should also be consistent. Technology-neutral policies which apply across devices and access technologies as well as across comparable applications are more efficient and sustainable in a dynamic environment. Where possible, interoperability of technologies for protecting children online, such as parental controls, should be encouraged in order to facilitate adoption and foster innovation.

Coherence

Policies which aim at the systematic promotion of mutually reinforcing policy actions across all public and private stakeholders create synergies which can help to achieve defined objectives. A prime example is awareness raising and education for children and their parents as well as other targeted groups such as educators, social workers and other trainers which is assured by various public and private stakeholders. The US Online Safety and Technology Working Group maintains that more inter-agency co-ordination, public awareness raising, and public/private sector co-operation are needed to improve the effectiveness of online safety education at the federal level (OSTWG, 2010, p. 6). The challenge is to convey coherent information so as to avoid contradictory advice and to link awareness raising effectively to other policy measures, such as guiding parents on parental controls.

Evidence-based policy

There is a growing consensus among countries that a systematic approach to evidence-based policy making is needed in order to determine policy priorities and maximise the protection afforded by national policy without unduly reducing the opportunities and benefits of the Internet for children. However, national policies are rarely formulated to create a virtuous cycle of evidence-based policy making based on the measurement of risks and impact assessment, with performance evaluation leading to continuous improvement. This may be due to the fact that this is both a complex policy area and an emerging field of research and policy attention.

Measurement of risks

The formulation of a policy which corresponds adequately to the reality of threat scenarios for children[51] relies essentially on the effective measurement of risks (Livingstone and Haddon, 2009, p. 22). A number of countries (*e.g.* especially European countries assisted by the EU's Safer Internet Programme, Australia, Canada and New Zealand) are surveying risks for children and young people online more systematically, both qualitatively and quantitatively. Indicators are essential for developing evidence-based policies for the protection of children online, including setting priorities. However, relevant indicators are not available for all countries and for all risks. A national repository is a possible way to survey available data across all sources systematically. Harmonisation of methodologies and definitions could be pursued in order to increase the usefulness and relevance of data for the policy making process.

Where appropriate, international co-operation would benefit from more consistent indicators of the prevalence of risk. This would facilitate international comparability and therefore help anticipate trends and identify best practices across borders. The inclusion of the protection of children online in existing OECD model surveys is a possible way forward, together with the development of specific indicators that build on existing data collections (such as hotline reports, statistics or regulators' complaints).[52]

The development of a measurement toolkit that would provide policy makers with a list of indicators and associated methodologies and definitions judged essential for developing policies for the protection of children online could be a practical international initiative to foster evidence-based policies and support national efforts for the protection of children online.

Policy impact assessments

Impact assessment (IA) is a method of evidence-based policy making (OECD, 2002, p. 44; 2007b, p. 5) which can systematically assess the problem of conflicting policy objectives and enhance the precision of policy measures. IAs are an established tool for improving policy making which emphasises the quantification of benefits and costs. They should be based on evidence, incorporate up-to-date research on the actual prevalence of risk, and determine realistic targets for subsequent evaluation.

Governments could issue IA guidelines for policies to protect children online, to be followed by private-sector organisations when they draw up self- and co-regulation. Such guidelines would detail the scope, content, accepted methodology and required evidence. Although the requirement to conduct such assessments places an upfront burden on public- and private-sector stakeholders, it is an acknowledged means of enhancing the precision of policy making. Further, it supports transparency, accountability and policy acceptance.

Performance evaluation

Performance evaluation offers policy makers a reliable way to learn about achievements, failures and the need for adjustments. It should be built more systematically into policy to protect children online in order to enhance policy effectiveness.

While voluntary commitments by the private sector have become a significant pillar of many countries' efforts to protect children online, it would be good practice for self- and co-regulation initiatives to include independent evaluations as a mechanism to monitor compliance and to enhance the effectiveness, transparency and accountability of private-sector stakeholders.

International co-operation

There is a common understanding across countries that international and regional co-operation is important in order to address the challenges of child protection in an inherently global medium such as the Internet. Intergovernmental organisations at international and regional level (APEC, CoE, ITU, OECD, WSIS/IGF, etc.), and in particular the European Union, have therefore initiated work within their remit (see Table 2). International efforts in this area are relatively recent and thus relatively unco-ordinated.

Ensuring international dialogue and consistency

When intergovernmental organisations are working in parallel, with different perspectives and sometimes overlapping mandates, they should ensure that their work is not duplicative and that their outcomes are mutually reinforcing. Fostering information exchange and dialogue between international organisations that play a role in protecting children online is essential.

As they are at the domestic level, inclusiveness and co-ordination are essential to successful international co-operation. Finding ways to involve all relevant international stakeholders and to co-ordinate the work of different actors in international organisations active in this field is a challenge. There is currently no established international platform dedicated to the protection of children online that would serve these functions and reflect all international activities.

In order to close this gap, countries, intergovernmental organisations and international stakeholders could decide to meet regularly with all relevant national stakeholders and international bodies. Such an event could provide a platform to foster consistency among initiatives planned by international organisations and to facilitate the sharing of best practices and experience across national stakeholders. A good example at regional level is the Safer Internet Forum, an annual event at the EU level on safer Internet issues, which has become an important reference for the dissemination of information on research, activities and policy efforts.

Cross-border sharing of information and resources and capacity building

The sharing of experience and best practices at the policy level is a shared objective. International policy guidance, involving governments, business and civil society, is an important yet underutilised means of conveying evidence-based lessons learned and best practices on a wide array of topics, such as programmes and resources which have proven effective in addressing issues concerning a particular age category.

Another key area for international co-operation is capacity building, whereby advanced countries or regions assist other countries in the development of their national policies, taking national specificities into account. For example the Council of Europe's Global Project on Cybercrime supports countries across the globe in their efforts to protect children against sexual exploitation and abuse, in line with the Convention on Cybercrime (CETS 185) and the Convention on the Protection of Children (CETS 201). Also, the APEC 2010 initiative, led by Australia, aims to train law enforcement agencies in the APEC region and build the capacity of APEC law enforcement agencies to respond effectively and offer greater protection to children from cyber-safety threats.

Finally, collaboration at the international level and with various stakeholders can help ensure commitment and greater visibility (*e.g.* Safer Internet Day) and the sharing of successful educational and awareness-raising campaigns where appropriate (ACMA, 2009, p. 95). A common understanding of what is positive online content for children and the sharing of positive online content for children among suppliers and across countries would help expand the range of suitable content for children.

Laying the empirical foundations for international evidence-based policy

Comparable information about national situations and policies is needed to stimulate efforts within countries. Countries should harmonise their statistical frameworks in order to lay the empirical foundations for the international comparability of risk prevalence and policy efficiency. An important starting point would be common definitions of risks and children's age groups. As an input for the effective measurement of risks, this would not require countries to modify their culture or policy approach to the protection of children online. Indicators do not have to reflect national legislations accurately. ITU work to devise a Child Online Protection Statistical Framework and Indicators (ITU, 2010b) is worth noting.[53] The OECD could introduce the protection of children online in its work on the measurement of the information society and as a specific module in its model surveys. Finally, the creation of a repository of official and semi-official statistics or the regular collection and comparison of national official and semi-official statistics could be a further means of improving the accessibility of available empirical data.

International networks and strategic partnerships at operational level

Existing international networks of hotlines and awareness centres can foster co-operation and co-ordination at the operational level and create synergies through the sharing of best practice, information and resources. Governments should promote and expand the networking of national organisations, including law enforcement, dedicated to the protection of children online and strengthen effective international networks at policy and operational level.

While countries are unlikely to align their definitions of what is illegal or inappropriate content for children, a common baseline of the types of content commonly regarded as off limits for children could be developed. The incompatibility of national policies on illegal and child-inappropriate content does not prevent international efforts to collaborate in labelling and content rating which can be tailored to national views and used as input for parental control technologies. National policies could benefit from effective international content labelling schemes which would provide additional information on the nature of content, such as the presence of violence.

Public-private partnerships involving several countries can develop policy responses which several countries might more easily be able to monitor and assess jointly than in isolation. Such initiatives may also be more cost-effective for private-sector operators than constellations of unco-ordinated parallel actions carried out in various countries. The joint promotion of regional self- and co-regulatory frameworks among major operators or across specific services categories can help achieve new, and/or consolidate existing, commitments to improve the overall level of protection of children online. For example, two self-regulatory initiatives involving mobile network operators and operators of social network sites in the EU have been concluded recently to the benefit of all participating countries. Working together towards common standards with market players such as Internet search engines, Internet advertising networks and other intermediaries who have proven their commitment to protect children online could produce a wider regional or even international impact on the enhancement of the protection of children online.

Whether the creation of suitable content for children is left to the market and private initiatives or supported by governments, a common understanding of what is positive online content for children among all stakeholders would help to introduce quality standards and could be used to encourage self-assessments of websites for children. It would facilitate the development of incentive-based policies to stimulate supply and demand. Private companies could then decide to adhere to this definition or pursue different content strategies for child audiences. Websites that are safe for children could be indexed and linked to create a network of varied online content for children (a whitelist) and provide a useful tool, especially for small language communities.

ANNEX I - DESCRIPTIVE OVERVIEW OF POLICIES TO PROTECT CHILDREN ONLINE

Introduction 52
Regional policy frameworks and national strategies 52
Legal measures 54
Self- and co-regulatory approaches 59
Community and acceptable use policies 63
Technical measures 64
Awareness raising and educational measures 71
Positive content provision 73
International co-operation 74

Introduction

This annex is a descriptive overview of policy responses to address these risks, including measures taken or planned by governments, business and civil society at domestic, regional and international levels.

This annex does not intend to provide an inventory of all initiatives carried out worldwide to protect children. It rather provides an overview of trends across governments and of major efforts carried out by business and civil society, highlighting commonalities and differences across countries with respect to policy measures and challenges. Its content is based on available research and on the responses to the APEC Questionnaire on Children Protection Online circulated in April 2009 to APEC and OECD members.[54]

It is structured to first describe regional policy frameworks and national strategies that have been developed to protect children online in a co-ordinated manner. It then provides an overview of the various types of policy initiatives adopted or encouraged across countries: legal measures and its effectiveness, self- and co-regulatory approaches, community and acceptable use policies, technical measures, awareness raising and educational measures, positive content provision and international co-operation. Where possible, an overview of the lessons learned is provided.

Regional policy frameworks and national strategies

Regional policy frameworks

Both the Council of Europe and the EU have devised and developed policy frameworks to protect children online. In some respects these overlap and reinforce each other; in other respects they are distinct and supplementary.

The Council of Europe has adopted a number of non-binding instruments with the aim to ensure a coherent level of protection for minors against harmful content and developing children's media literacy skills. Member countries are called on to develop information literacy and training strategies which effectively empower children and their educators.[55] A subsequent Recommendation to member countries for specific measures to protect children against harmful content and behaviour and to promote their active participation in the new information and communications environment sets out guidelines on providing safe and secure spaces for children on the Internet, the development of a pan-European trustmark and labelling systems, and skills and literacy for children, parents and educators.[56] As regards the content created by children on the Internet, the Council of Europe declared that there should be "no lasting or permanently accessible record" detrimental to their dignity, security and privacy in their future lives.[57]

The EU introduced harmonized legislation pertaining to child protection online. Most notably, the 2007 Audiovisual Media Services Directive expands the protection of minors from inappropriate content and commercial communication to on-demand audiovisual services delivered over the Internet.[58] For all online services, the 1998 and 2006 Recommendations on the protection of minors and human dignity encourage awareness raising and media literacy, identification of quality content for children, as well as industry efforts in order to make the Internet a safer place for children in member states.[59]

With the Safer Internet Programme (SIP), the EU assumes a regional lead in stimulating policy making and implementation as well as co-operation between its member states.[60] Since 1999, the European Commission promotes various initiatives under SIP to make the Internet a safer place for children. The programme, which entered in its third phase in 2009, has been instrumental in funding pan-European networks and national initiatives in the EU and in setting up the international hotline network INHOPE and

European network of awareness centers INSAFE (see below, international co-operation). Under the same umbrella, the Safer Internet Forum is an annual conference where representatives from law enforcement authorities, industry, child welfare organisations and civil society as well as policy makers discuss specific topics related to child safety online. A EUR 45 million budget supported SIP 2005-2008. SIP 2009-2013 will allow for EUR 55 million to be invested in public awareness measures (48%), fight against illegal content (34%), addressing illegal conduct online (10%) and establishing a knowledge base (8%).[61]

National policy frameworks

Several OECD countries have devised national strategies (*e.g.* Australia, Canada, and United Kingdom) and developed policy frameworks (*e.g.* Japan) which address child protection in the light of new challenges raised by the Internet, combine and co-ordinated measures and involve various stakeholders.

One of the earlier strategies is the 2000 Canadian Cyberwise Strategy to Promote Safe, Wise and Responsible Internet Use, which is not any longer actively pursued. The strategy excluded the adoption of new legislation and placed priorities on awareness, shared responsibilities according to the roles of stakeholders, effective enforcement mechanisms and consultation between the public and the private sector and their counterparts in other countries.[62]

With respect to inappropriate content, the US generally supports an industry-led, self-regulatory approach reinforced by enhanced consumer awareness and the widespread availability of consumer empowerment technology whenever possible.[63] Therefore, parental controls and public-private partnerships that emphasize self-regulation are often employed in strategies to protect minors from online dangers. Highly targeted legislation has been passed for specific issues, for example in the field of children privacy protection online[64] and in order to avoid children accidently stumbling over explicit content.[65]

Under Australia's 2008 Cybersafety Plan, funding of AUD 125.8 million (approx. EUR 81.2 million) over four years was committed towards, among other things, cyber safety education and awareness raising activities (including the creation of education resources and expansion of a national outreach program under the ACMA's comprehensive Cybersmart program), law enforcement and a content filtering scheme which will become mandatory for Internet Service Providers. As part of the Cybersafety Plan, a Consultative Working Group on Cybersafety, a Youth Advisory Group and research will inform the government on cyber safety issues.

The Bristish government accepted the recommendations of the independent report "Safer Children in a Digital World"[66] ("Byron Review") which led to the establishment of the new United Kingdom Council for Child Internet Safety (UKCCIS) – an organisation consisting of 150 stakeholders tasked with the development and implementation of a Child Internet Safety Strategy. Its first strategy was published in the end of 2009 and concentrates on creating a safer online environment for children, empowering parents, carers and trainers to help children and young people stay safe online, and inspiring safe and responsible use and behaviour.[67] The work will be updated by evidence and progress will be evaluated through research together with an expert research panel; UKCCIS provides and updates certain industry guidance[68] compliance with which it will be reviewed.

Japan's national policy approach has led to the adoption of the "Act on Development of an Environment that Provides Safe and Secure Internet Use for Young People" in June 2008. This law promotes the furtherance of efforts to protect children from illegal and harmful information on the Internet, for instance, by making it obligatory for mobile phone operators to provide filtering services, and also makes provision for initiatives such as the promotion of improved ICT literacy for citizens.[69]

Legal measures

Legal measures to protect children online vary according to their *degree of specificity* with respect to the Internet (*i.e* legislation that applies to all media including the Internet versus Internet-specific legislation) and with respect to the targeted population(s) (*i.e.* legislation that aims to protect all citizens, including minors versus legislation that specifically aims at protecting minors). National laws also vary according to *the risks* that they aim to address (*e.g.* content-related risks, consumer risks, privacy and information security risks) and to the *type of requirements* they specify (*e.g.* content rating scheme, parental consent requirement, or mandatory filtering).

Since many risks that children may encounter online have an offline expression, general laws apply and most countries subscribe to the principle that what is illegal offline is also illegal online. This report, however, focuses on specific legislation and regulation of child protection online but does not attempt to give a full inventory and analysis of general laws, such as criminal, civil or consumer protection laws which do not take a child-centered approach. Neither does the report cover national strands of case law.

Some countries, such as Japan, Korea and Turkey, have issued new and/or comprehensive legislation addressing specific risks children often face online as a reaction to local situations.[70] These legislative measures addressing threats for children are often included within broader laws that aim at regulating the Internet. This new breed of laws tends to tackle content- and contact-related risks together and mandates complementary technical safeguards.

New legislation is also used to patch specific areas of concern such as the US law on misleading domain names[71] and the update of the French criminal code to make the distribution of "happy slapping" images and videos a criminal offence.[72]

Legal approaches to sexual exploitation and abuse of children on the Internet are not examined in this annex but addressed in the study carried out by the Council of Europe.[73]

Legislation on content-related risks

Content laws and regulations exist in most of the countries surveyed and commonly there are categories for illegal content and child inappropriate or unsuitable content. Thus, the first threshold is illegal content which, according to the local laws, is unsuitable to be publicised to a general audience. The second threshold is child inappropriate content as specified in local laws where the type of content is deemed harmful for child audiences.

Only a very vague common set of content types is typically considered illegal across countries, *i.e.* depictions of child sexual exploitation, bestiality, extreme forms of pornographic violence. There is even much less consensus and less clarity regarding the definition of child inappropriate content across countries.

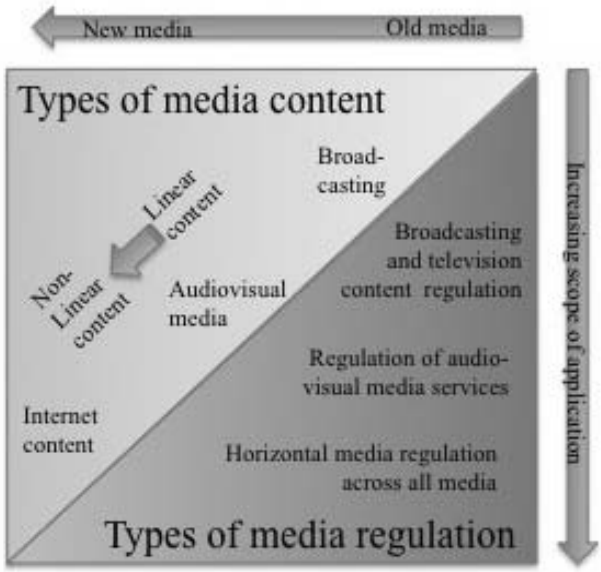
Legislative measures against illegal or child inappropriate content can take the form of *i)* general laws; *ii)* media content regulation, applying either to specific media services or across all media platforms; and *iii)* specific legislative measures pertaining to the Internet.

Legislation pertaining to illegal content is often general laws, applying across all media including the Internet, such as for example, the UK Obscene Publications Acts prohibiting the publication of indecent or obscene material without regard to the audience, medium or the format.

The regulation of child inappropriate content often has its origins in television regulation, which some countries (gradually) expanded in order to capture television-like formats (linear) transmitted over the

Internet and certain on-demand services, with a few countries abolishing any distinction between old and new media (*i.e.* horizontal content regulation). Figure 12 illustrates the different types of media content, from traditional to new media content, the regulatory regimes, and the gradual expansion of their scope of application to cover certain types of media under content regulation. For example, following EU harmonized rules of the 2007 Audiovisual Media Services Directive, member states are about to introduce new rules in order to protect minors from audiovisual media services, which might seriously impair their physical, mental or moral development.[74]

Figure 12. Types of media regulation



To tackle child inappropriate content, many countries (*e.g.* Australia, Germany, Korea and New Zealand) have adopted media content regulation based on age limits and access restrictions and applying horizontally across all electronic information and communications platforms.[75]

Content passed on via individual data exchange (*e.g.* e-mail attachment, mobile to mobile, file transfers via instant messenger) is beyond the scope of such media regulation.[76] This gap in the legislative responses to content-related risks for children appears to be present in all countries which leaves a question mark as to whether this is justified in the light of the widespread use of these technologies by children. Individual electronic communications however is protected against censorship by the right to privacy of personal correspondence or the confidentiality of communications vested by countries' constitutions.

Countries with content regulation maintain content rating and labeling frameworks with minimum categories for adult content (*e.g.* rated for 18 year olds, "R18+") and illegal content (*i.e.* refused classification "RC") and allowing for further granularity as required.[77] Official classification is carried out by public bodies and regulators (*e.g.* Australian Classification Board) or is sometimes delegated to co-regulatory bodies (*e.g.* in Germany and the Netherlands).[78] Self-declaration schemes where the content originator is rating and permanently tagging its content is growing (see below under Content rating systems).

Online content regulations and accompanying measures are always targeting the content provider but also increasingly so are Internet intermediaries that give access to, host, transmit and index content originated by third parties such as Internet host service providers, Internet access providers or search

engines.[79] In particular, intermediaries are often the only entities capable of enforcing local content rules against illegal content when the content originator is established abroad. In some countries (*e.g.* Australia, Italy, Japan, Korea and Turkey), competent authorities can request Internet host service providers under their jurisdiction, which are hosting prohibited content pursuant to local standards, to take down online content.[80] In many other countries, notice and take down procedures operate under voluntary agreements adopted by Internet intermediaries (see below self- and co-regulatory approaches).[81] In addition, a few countries have embarked on mandatory filtering schemes under which Internet service providers are required to block access to specific illegal content which is hosted abroad (*e.g.* Turkey, Italy with respect to child sexual abuse images and illegal gambling Web sites and in Germany where a law requiring the filtering of child sexual abuse images exists but is not implemented).

Notice and take down (NTD) policies require the Internet service provider which is hosting prohibited content, and sometimes links to such material, to remove the content or the links after notification.

Legislative prohibitions and restrictions of online content are generally not a stand-alone solution to child protection online but are often combined in various ways with access restrictions through technical and organisational measures. For example, technical measures to prevent minors from accessing child inappropriate content are sometimes required by law, such as filters, age verification systems or identity verification mechanisms (see below technical measures).[82] In addition, some countries (*e.g.* Korea and Spain) require operators and service providers to set up organisational structures to assist online child protection efforts, such as by allocating designated personnel and establishing information duties.[83]

Finally, in some countries, content legislation is limited as a consequence of constitutional requirements vesting highest value in free speech rights. In the US, for instance, several attempts to introduce online content regulation with the aim to protect minors were found unconstitutional.[84] The US Children's Internet Protection Act (CIPA) of 2000 therefore concentrates on schools and libraries which in order to continue to receive a type of federal funding must certify that they have an Internet safety policy and technology filtering Internet access and blocking pictures that are obscene or harmful to minors. In Canada, the Criminal Code provides for a judicial take-down system of illegal content.[85]

Legislation on contact-related risks

There is a very diverse body of legislation pertaining to contact-related risks for children and loopholes where acts committed using electronic communication and information systems challenge countries' legal systems.[86] Where children are harmed by others, certain acts of online contact can be punishable as a criminal offence.

A few countries, namely Australia, France, Ireland, Japan, New Zealand, Norway and the United Kingdom, have already specific provisions in place criminalizing cybergrooming. The implementation of similar criminal offences is planned in the Netherlands and Sweden in the course of implementing the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse of 2007.[87] In Japan, the use of Internet dating sites to arrange dates with minors is a criminal offence.[88] In the United States the KIDS Act of 2008[89] requires convicted sex offenders to provide their "internet identifiers" to the sex offender registries and this bill also establishes a system by which social networking Web sites can cross-check the list of their users against this database.[90]

Online harassment and cyber-stalking, depending on the circumstances, may meet the definition of criminal harassment, for example, in the criminal codes of Canada or the United Kingdom. In the United

States and in Australia, stalking or harassment laws make specific reference to electronic forms of communication.[91]

Cyberbullying is a form of online harassment and can be punishable as such; however, where perpetrators are themselves children, legislators may prefer regulation in terms of educational policy rather than criminal law. For example, legislation enacted in many US States introduces rules against cyberbullying in the school environment and/or requires school authorities to adopt prevention policies.[92]

In order to mitigate contact-related risks for children online, mandatory monitoring of chats and bulletin boards has been introduced in some countries, for example in Sweden,[93] and in Japan on-site age verification is a legal requirement for online dating Web sites.[94] However, countries more often encourage voluntary commitments with respect to monitoring and moderation, rather than imposing an obligation (see section below on Community and acceptable use policies). Finally, in Korea, the implementation of an identity verification system is a legal requirement placed on Internet Web sites of a certain size and although this scheme does not herald child online protection as an objective, it can help to prevent and where necessary to investigate online contact-related risks for children.[95]

Legislation on online consumer risks for children

Three strands of legislation commonly apply to online consumer risks for children, *i.e. i)* private law, and *ii)* consumer protection laws alongside *iii)* legislation with the specific objective of protecting children against these risks. Commonly, in private law, underage users do not have the legal capacity to enter into contracts. Consumer protection laws, such as national anti-spam legislation, lay down conditions which also but not exclusively benefit child users. Specific legislative measures against typical child consumer risks apply offline and/or online and are tailored to children's ability to recognise, understand and critically assess commercial communication, services and offers.

Many countries (*e.g.* Germany, Korea, Turkey, United Kingdom and United States) maintain underage gambling prohibitions and in the United Kingdom gambling Web sites may only get a license if they can show that they have a robust age verification mechanism in place. Australia maintains an interactive gambling prohibition *per se*.[96]

With respect to online advertising directed at minors, two contrasting models prevail with countries regulating certain aspects of online advertising to children on the one hand and countries' reliance on industry self-regulatory schemes on the other hand.

The EU is an example for the first model, where harmonized rules for audiovisual media services provide a range of advertising restrictions, including specifically protecting children. Apart from the general ban of cigarettes and tobacco advertisements it is prohibited to promote alcoholic beverages aiming specifically at minors.[97] On the premise that commercial communications in the relevant services should not cause physical or moral detriment to minors, practices which exploit, for instance, minors' inexperience and credulity are prohibited. Audiovisual commercial communications must be readily recognisable and product placement in children's programmes, including on-demand audiovisual content available on the Internet, remains prohibited.[98]

Scandinavian countries have the most elaborate rules on Internet marketing aimed at children and minors residing in the Nordic markets. All marketing online has to comply with legal standards which require, in particular, that marketing be recognizable by children and correspond to its target group's stage of development, that children must not be invited to make purchases or agreements via the Internet and that "advergaming" is banned, as is the provision of prizes given if children take part in online activities.[99]

Advertising for child inappropriate content to children is banned in Korea.[100] The US CAN-SPAM Rules, including the Adult Labeling Rule, requires warning labels on commercial e-mail containing sexually oriented material in order to place a bumper between x-rated e-mail and children.[101]

Legislation on privacy and information security related risks for children

Information privacy and information security risks for children are with a few exceptions subject to general data protection rules and criminal law rendering some information security risks a criminal offence.

In European countries, the collection and processing of personal data must be authorized by law or informed consent and has to conform to further data protection principles.[102] Parents' informed consent is required until the child has developed the capacity to fully understand the extent of such determinations which leaves certain ambiguities with regards to the age until which parents must give their informed consent on behalf of their children which may vary from child to child and across scenarios.[103] The joint working party of EU Data Protection Commissioners (so called Article 29 Working Party) acknowledges the participative right of a child which would require him or her to be informed and consulted and even be part of a decision on the processing of his or her personal information depending on their level of maturity, which is adding further complexity to the legitimisation of the processing of children's personal data.[104]

The US provides an example of a very targeted legislative response with the Children's Online Privacy Protection Act (COPPA) and corresponding Rule.[105] COPPA places obligations on operators of Web sites directed at children under 13 or where personal information of children under 13 is knowingly collected.[106] In order to determine whether a Web site is directed at children, the Federal Trade Commission takes into account a range of criteria, including the subject matter; the audio or visual content found on the site; the age of any models depicted on the site; the language used on the site; the presence of advertising on the site; other empirical evidence regarding the age of the actual or intended audience, such as whether the site uses animated characters or has other child-oriented features. COPPA only applies to a given general-audience Web site which is not directed at children under 13 where the operator is knowingly collecting personal information from these children. COPPA's objective is to give parents control over what information is collected from their children online by requiring parental consent. The available procedures to establish the authenticity of the parental consent (*i.e.* sending an e-mail from a parents e-mail account provided at the time of signing in, the provision of the parents' credit card details, a written consent form from the parent, or a telephone call from parent) have been criticized for being easy to circumvent (Bartoli, 2009) and workable alternatives have not yet emerged. The same problem arises in Europe where parental consent for the collection and processing of children data is required although no easy-to-implement and reliable mechanism to establish such parental consent is available.

The overall effectiveness of data protection frameworks when applying to children's personal information ought to be questioned (see below Effectiveness of legal measures).

Information security risks stemming from spyware or malware are cybercrimes and are a criminal offence in countries which have ratified the Council of Europe Cybercrime Convention.[107] There is no specific legislation to mitigate information security risks for children.

Effectiveness of legal measures

Countries report unanimously that legal safeguards are under considerable strain for reasons that are inherent to the Internet as a global and highly dynamic information space.

For instance, content regulation is on a stand-alone basis inadequate to deal with material stemming from abroad and the same material can be perfectly legal in one country and classified in another. The vast

amount of content generated online each minute poses an additional challenge to content regulation and existing content rating and classification systems would be outpaced if they were to follow up all rating requests. For example the video sharing platform YouTube reports that every minute 20 hours of video is uploaded.[108] Consequently, countries have embarked on various strategies that help uphold local content regulation which involve Internet intermediaries. In some countries Internet service providers are legally obliged to comply with state authorities' take-down notices (*e.g.* Australia, Italy, Japan, Korea, and Turkey), in many other countries 'notice and take-down procedures' operate under voluntary schemes (*e.g.* Denmark, United Kingdom). Increasingly, Internet intermediaries deploy technical filters which in very few cases is a legal obligation to block access to specific types of illegal content online (*e.g.* Italy, Turkey, and proposed in Australia) but in the majority of cases on the basis of voluntary commitments by the industry.

The main challenge for the legal protection of minors' personal data lies in the effective implementation and enforcement of existing rules given the ubiquity of online activities involving children's personal data today. Both legal approaches practiced, *i.e.* general data protection laws and child specific data protection laws (*i.e.* COPPA), incorporate safeguards (*e.g.* consent and privacy notices) that are unlikely to be more effective for children and their parents than overall. The role and limits of the consent requirement in privacy protection has been discussed elsewhere in OECD[109] and concerns persist in relation to the requirement of parental consent. The requirement of parental consent seems to be difficult to implement since so far there are no easy mechanisms for gathering verifiable parental consent.[110] In Canada the Children's Online Privacy Working Group has published a discussion paper presenting various regulatory options to enhance children's online privacy which nevertheless rely on varying consent requirement schemes.[111]

Websites targeting child audiences must make a default assumption about their users and make the collection of children's personal data dependent on obtaining parental consent. Parental consent requirement would not be effective if children lie about their true age either with or without the approval of their parents. Conversely, general online services are used by adults and children, however, the age of Internet users is notoriously difficult to assess. The application of laws across borders is also a source of challenge. For example, many British children use US-based online services and are therefore subject to the US rather than to British privacy rules. Children and their parents may find it difficult to disregard in the change of jurisdiction and potential consequences for enforcement. Privacy laws are also not self-enforcing which is why many countries support self- and co-regulation in addition to or instead of privacy legislation.

With regards to consumer-related online risks many offline safeguards fail in the online environment: for example, face-to-face offline contacts give an indication of the person's age but it is easy for children to pose as an adult online through lack of efficient age verification mechanisms. Online age verification systems which are not to be deployed overall but for specific services only have shortcomings, which make them cumbersome to use and leave scope for circumvention.

Self- and co-regulatory approaches

Several countries, as well as the EU, recognise that self- and co-regulation plays an important role for the protection of children online and consider voluntary commitments as a key component of national policies. Business-value these instruments as a means to demonstrate social responsibility and commitment. Therefore, the protection of children online is a prolific area of self- and co-regulatory initiatives which can take various forms and are sometimes referred to as codes of conduct, industry guidelines and best practices.

The spectrum of co-and self-regulatory initiatives is wide and boundaries between the two concepts are not clear-cut, but as a rule of thumb, co-regulation, on the one side, is characterised by a combination of government and private regulation whereas self-regulation on the other side is a purely voluntary commitment on part of the private sector without any government involvement.[112] Modern forms of governance, such as public-private partnerships, are at the intersection of co-and self-regulation, as the government is a party to the negotiation of a voluntary commitment of private stakeholders. Often the result bears the characteristics of self-regulation but the process, leading to the adoption of the initiative, was actually catalysed in a public-private partnership.

Countries deploy various strategies to encourage self-and co-regulation such as by *i*) making explicit reference to these mechanisms in legislations; *ii)* giving a mandate to regulatory authorities to negotiate with stakeholders voluntary commitments; *iii)* creating platforms for stakeholders to convene; and *iv)* stirring problematic areas by threatening to resort to "command and control" style regulation. The Children's Online Privacy Protection Act (COPPA) in the United States, for instance contains a statutory safe harbour provision -- if a website participates in a safe harbour programme, it is afforded a presumption of being COPPA compliant if the website is in compliance with the requirements of the authorised safe harbor.[113] *Public-private partnerships* where voluntary agreements have been brokered with strong public sector involvement (detailed below) led to recent self-regulatory initiatives involving mobile network operators and operators of social network sites in the European Union and the United States.[114] It appears that in particular public-private partnerships are successful in delivering effective voluntary commitments by industry with the aim to protect children against harm online.

Existing models can be classified according to whether *i)* it is co-regulation or self-regulation; *ii)* it is an industry led commitment or it involves all relevant stakeholders; *iii)* it applies to one country or represents a regional agreement; and *iv)* it is a single group's standard or collective agreement.

In online services and new media, self- and co-regulation is widely deployed in order to mitigate risks for children on the Internet and is often woven into national policy frameworks. Countries and the EU actively encourage self- and co-regulation in their laws and through public-private partnerships. Across sectors, activities concentrate primarily on three areas: *i*) content-related risks online; *ii*) online marketing to children; and *iii*) the protection of children's personal data. However, the protection vested by voluntary codes is not without gaps and the lack of harmonised protection principles produces disparate outcomes even within a given country.

When assessing self- and co-regulatory schemes, the quality, impact and the effectiveness can vary significantly depending on a number of general factors such as *i*) how inclusive are the rules that have been developed; *ii)* if transparency and accountability is achieved; and *iii)* whether the rules are binding; *iv)* enforceable; and *v)* subject to evaluations. For example, the EU Safer Internet Programme supports industry self-regulation regimes where they are broadly accepted by stakeholders and provide for effective enforcement.[115]

The examples below provide a brief overview of the major self- and co-regulatory initiatives with respect to mobile communications, social network sites, online games, online advertising and illegal and child inappropriate content.[116]

Mobile communications

Adopted in 2007, the European Framework for Safer Mobile Use by Younger Teenagers and Children describes principles and measures to be implemented at the national level, including access control for adult content; awareness-raising campaigns for parents and children; the classification of commercial content according to national standards of decency and appropriateness; and the fight against illegal

content on mobiles.[117] The implementation of the framework, into national codes of conduct has been independently monitored showing that in 2009, two years after its inception, 22 member states have codes that show a high level of alignment with the framework, and mobile operators self-report a very high or high level of compliance.[118]

In the United Kingdom, all of the mobile networks operate an adult bar which is turned on by default to block access to adult content offered over the mobile phone network. In order to have the adult bar removed it is necessary to go through an age verification process with the network operator. Similar measures are taken by mobile telephony networks in the US and other countries. It is however also possible to access child inappropriate content available on the Internet with a mobile phone and the practice varies as to whether mobile network operators provide network level filters and where available also whether filters are turned on by default for all customers or upon request.

The Australian Mobile Premium Services Code covers *inter alia* advertising mobile premium services to minors.[119] The Code forbids advertisement for mobile premium services which is specifically targeted at persons below the age of 15 years and where the advertisement of a mobile premium services is likely to attract minors to use that mobile premium service it requires the warning "If you are under 18 you must ask the account holder before using this service". The Code also contains provisions on mobile commerce by requiring that customers provide two confirmations of their purchase.[120] The confirmations provided by the content supplier must also clearly include the name of the subscription service, any sign up cost, the basis for calculating the charge, instructing the customer how to subscribe and include details of the help line.

Social network sites

In the United States, public-private partnerships that emphasize self-regulation are often employed in strategies to protect minors from online dangers. For example, the Attorneys General Multi-State Working Group on Social Networking and two of the largest social network sites issued joint statements committing these social network sites to better protect children through the application of key principles.[121] Based on recommendations from the Attorneys General and online safety advocates, the services developed more nuanced privacy settings and information practices about online risks for children. Concrete changes introduced for example to the service of MySpace, aim to prevent children under 14[122] from signing up and protect minors aged 14 and above from exposure to inappropriate content and unwanted contact by adults.

Major social networks operating in the EU adopted Safer Social Networking Principles[123] developed in consultation with the European Commission, NGOs and researchers and submitted self-declarations in which they provide details about how their services relate to the principles.[124] The principles aim to limit the potential risks of social networking sites for under 18s.[125]

Examples of concrete measures taken are the introduction of reporting mechanisms such as an easy-to-use and accessible "report abuse" buttons, the improvement of default privacy settings and controls for profiles of users under 18, and finally preventing users below the age the service is targeting, from registering.[126] A first independent assessment of the implementation of the Safer Social Networking Principles has been conducted where the compliance of social network sites with their respective self-declaration has been assessed.[127] The compliance varies by provider with two social network sites excelling, but the findings of the majority is good or fair compliance leaving scope for improvement.

Online games

The Pan-European Game Information (PEGI) Online Safety Code of 2007 is another example for a European-wide self-regulation scheme which aims at providing a minimum level of protection of young people in the online gaming environment.[128] Signatories to the code commit themselves to adhere to a

content rating system, to remove inappropriate material from their site and to set up community policies and reporting mechanisms that help to ensure appropriate behavior among users. Further, the code includes provisions regarding advertising which promote separation and fairness principles and in particular that all advertising must correspond to the age of the audience the online gaming website is targeted at.

Online advertising

Self-regulation produced a great number of industry standards to protect children from certain online marketing techniques and children's personal data (*e.g.* International Chamber of Commerce's (ICC) Advertising and Marketing Communication Practice, the International Advertising Bureau UK and US codes, the Federation of European Direct and Interactive Marketing (FEDMA) code and many more).[129] These instruments either apply to all marketing practices or only to online marketing and they cover marketing to adults and children or specifically to children.[130] Schemes vary significantly with respect to the age up to which children are protected (*e.g.* sometimes only applying to children under the age of 13 or 14) and the actual protection vested in addition to the available legislation.[131]

At the national level, there are codes, either voluntary or complementary to legislation, of marketing organisations and also content providers, tackling the marketing for food and drink products high in fat, sugar and salt (so called HFSS food) to children. These instruments can apply to audiovisual media and on-demand services or to all Internet services under its scope.[132]

The contribution of self- and co-regulation to the protection against child-specific consumer risks online is beyond question. The landscape of voluntary codes, however, is fragmented along the boundaries of industries, national borders and through membership of the respective umbrella organisation and, despite many parallels and overlaps, gaps in protection remain. New online marketing techniques such as embedded advertising, extensively branded websites and behavioral targeting on websites directed to children, are not yet sufficiently taken up under voluntary schemes.[133] The Article 29 Working Party is of the view that advertising network providers "should not offer interest categories intended to serve behavioural advertising or influence children" because of the difficulties to obtain consent in accordance with the laws and also taking into account the vulnerability of children.[134]

Illegal and child inappropriate content

The co-regulatory model where legislation is supplemented by voluntary agreement is favoured in a number of countries especially to address illegal and child inappropriate content.[135] Germany champions an approach called 'regulated self-regulation' where government recognized self-regulatory bodies implement content-related child protection standards.[136] The Australian Content Services Code developed by the Internet Industry Association (IIA) operates under the authority of Australian Communications and Media Authority (ACMA), which can ultimately enforce adherence to it.

Self- and co-regulation both play an important role in classifying and rating content. In Japan, for example, the Mobile Content Evaluation and Monitoring Association, the Internet-Rating Observation Institute (I-Roi), and the Rating and Filtering Liaison Council are self-regulatory bodies in charge of content rating within their remits. Positive content rating is used in Mexico where AMIPCI, the Mexican Internet Association, issues safety seals to websites without harmful content.

Voluntary self-labeling is used in connection with filtering software which recognises the label and thus blocks child inappropriate online content. Examples include the universally available ICRA label operated by the Family Online Security Initiative (FOSI) and the RTA (Restricted To Adults) label operated by the Association of Sites Advocating Child Protection (ASACP). Germany recently amended its media regulation on the protection of children in order to have content providers voluntarily label their

websites according to a classification scheme which would be capable of being interpreted by parental control software.[137]

Internet intermediaries such as Internet service providers and telecommunications operators which can technically remove problematic content have adopted self- and co-regulation codes and practices that help protect children online. In the Netherlands, for example, the Dutch government and leading host service providers agreed on a notice to take down code which sets forth guidelines to respond to unlawful and also undesirable content on the Internet and the way private parties erase this content.[138] German search engine operators developed a code of conduct with the aim of improving the protection of children and youths when using search engines where, for example, they commit to filtering indexed content from the search results.[139]

Community and acceptable use policies

Private policies play an increasingly important role to set rules for responsible and acceptable use of online services and their adoption is promoted in some countries in various ways.[140] Operators of IT networks, online platforms, mobile and Internet services can stipulate terms of use or encourage user community standards to contribute to the mitigation of online risks for children. Examples can be found in social networks, gaming, or photo and video sharing websites where they define inappropriate contents or behaviours and establish graduate sanctions against users who breach these rules.[141]

There are various scenarios. For example *i)* public institutions such as schools and libraries and other Internet access points implement their own policies; *ii)* self- and co-regulation agreements include the commitment to put community or acceptable use policies in place; *iii)* providers of online services and portals take-up community or acceptable use policies; and *iv*) online service contracts include terms of use.

School policies can be updated to cover certain risky online behaviours which can take place using the school's equipment. For example in many US states, cyberbullying laws require schools to adopt anti-harassment and anti-bullying policies or require school districts to devise model policies.[142] Similar measures can be taken for other public access points such as public libraries and also Internet cafes, which in order to be effective also require monitoring of compliance and reporting mechanisms.

Sometimes self- and co-regulation mechanisms contain the commitment to adopt acceptable use policies. One example is the PEGI Online Safety Code that requires community standards prohibiting illegal or offensive online behaviour and uploading of illegal or harmful content.[143]

Community and acceptable use policies are often maintained by social networks and other online communities. They detail the main acceptable user behaviour and content and can be enforced and sanctioned. Increasingly, the community of users is involved in flagging and reporting problematic content and behaviour, thus helping to self-police websites.

Terms and conditions of use laid down in a contract for communications services can be the basis for example to take down problematic content from customers. In Japan for example, industry groups have developed model contractual provisions to prohibit a number of problematic issues, including the dissemination of information relating to suicide.[144] When receiving notices of child inappropriate content, the Japanese helpline informs the Internet host service provider which can then enforce contractual obligations *vis-à-vis* its customers and take down the contested material.[145]

An additional tier for online safety in social networking sites and online communities, is the voluntary moderation by operators of interactive services for children. The United Kingdom Home Office published Good Practice Guidance for the Moderation of Interactive Services for Children (2005) and for the Providers of Social Networking and Other User Interactive Services (2008).[146] The 'Byron Review'

recommended developing these guidelines into an independent voluntary code of practice for the moderation of user-generated content, however, the United Kingdom Council for Child Internet Safety (UKCCIS) First Child Internet Safety Strategy issued in 2009 committed to update this guidance and for its members to adhere to it.[147]

Technical measures

Overview of technologies

Technical measures are an important element in child online protection policies. Technologies can be used to *i)* keep certain risks away from children (*e.g.* filtering technologies); *ii)* keep children out or, the reverse, admit only children to specific websites (*e.g.* age or identity verification systems); and *iii)* create child safe zones on the Internet (*e.g.* walled gardens).

This section will discuss filtering technologies and other technologies such as children's devices, age verification systems, content rating technologies and report abuse mechanisms. The following overview lists technical measures in the first column that help protect children online and illustrates their operationability at the various stages of the value chain of online services.

Figure 13. Overview of technical measures

Value chain	Content Originator	Web site/ online service	Internet service provider	Navigation & search	Internet access provider	End user terminal
Example	User uploading image	Social Network Site	Communications infrastructure operator	Search engine	DSL provider	Laptop, mobile phone
Children devises						Hardware restrictions, e.g little memory, no camera
Blocking		Preferences and privacy settings Web site specific measures			Blocking of Services e.g. of value-added mobile service	Parental controls block applications such as instant messaging, chat, video camera
Content rating and classification	Self-labeling, e.g. ICRA label	Peer-rating	Input for blacklist and whitelist filtering			
Technical filters		Web site level filters	ISP-level filtering (voluntary or mandated) based on blacklist	Filters (safe search, browser plug-in, child versions of search engines)	Filters, Activation of network or server based parental controls	Parental controls Filtering software
Age verification systems		Mandated or voluntary age verification system, e.g online gambling Web site			Mandated or voluntary age verification	
Report abuse buttons		Web site specific measure		Browser button linking to Internet hotline	Provider specific measure	

Filtering technologies

Filtering technologies encompass a whole range of tools that can block users from accessing content. They operate at various levels such as on the user's personal equipment, at Internet Service Provider (ISP) level or mobile operator level, and at search engine level. Each filtering technique has its strengths and limitations.

Methods

Filtering is based on *whitelists*, which block access to all Web content except when listed as suitable for the user, or on *blacklists*, which enable access to all Web content except when listed as inappropriate for the user.

The whitelist approach is recommended for younger children. Even though a lot of harmless content is not accessible, it is generally assumed that a safe environment is more important for young children than access to a large amount of information. Even though they might let through some undesirable content, filters based on blacklists are commonly deemed better for teenagers as they allow wider exploration of the Internet, thus responding to information and communications needs which increase with age.

Similar to whitelists, child safe zones, sometimes called "walled gardens", are Internet portals through which children can access a range of suitable websites and online services but cannot navigate away,[148] thus significantly restricting access or functionality.[149] The German service "fragFINN"[150] offers a 'smaller version' of the Internet where children aged 8 to 12 can navigate without facing potential threats or the disadvantages of current filter systems. An easy-to-install technical solution in the form of an Internet browser add-on ensures that children can only access websites included in a whitelist put together by a team of editorially independent media pedagogy experts. Other examples include video applications designed specifically for children, such as the Kideo Player from a US company and Totlol.com designed by an independent Canadian Web developer.[151]

Blacklists can be maintained based on some sort of pre-classification or generated dynamically through dynamic analysis techniques applied in real time.

Pre-classification can be based on official content-rating mechanisms or on lists of Web addresses (URLs). It can be human-based or computer-based and may be performed by vendors of content control software or by dedicated third parties[152] or by the content producers themselves.[153] Blacklists of legally prohibited content such as child abuse images are commonly maintained by law enforcement authorities (*e.g.* in Finland, Sweden) or regulatory authorities (*e.g.* Australian Communications and Media Authority (ACMA), Turkish Telecommunications Communication Presidency (TIB)) and, more rarely, by self-regulatory bodies (*e.g.* Internet Watch Foundation (IWF) in the United Kingdom). There are arguments for blacklists or other content classification not to be publicly available in order to prevent the content moving on to other URLs. Conversely, transparency of blacklists can also be conceived as a measure to enhance public confidence in the legitimacy of ISP-level filtering obligations and accountability of the governments.[154]

With dynamic analysis techniques, software applications determine in real-time, *i.e.* when the user attempts to view the page, whether the content should be blocked. They are potentially more effective in blocking newly published undesired content but the technology has shortcomings, such as allegedly throttling Internet connectivity speed and the potential to overblock, *i.e.* block uncontested content.[155]

In addition to blocking Web content, filtering technologies can also help address some contact-related risks such as child grooming or harassment, with applications that monitor chat or instant messaging for certain words or through text analysis tools. Text analysis technologies are more sophisticated than filters

for terms and character strings, since they are designed to automatically detect predatory, harassing, or otherwise inappropriate conversations on the Internet by using statistic-sampling, *i.e.* a method where statistically valid samples of representative text is collected and against which communications will be probed and assessed.[156] The technologies are still early in their development and though promising in many respects, it is unclear whether they can handle the complexity of multilingual, colloquially and conversationally diverse online communication.[157]

Some information security risks such as phishing scams or malicious spam messages can be addressed by filtering tools. There are many stand-alone solutions available but only a few suites which combine anti-virus and anti-spyware filters with child protection software. Internet browsers' preferences and security settings can also be adjusted to block pop-up and cookies, which would be a way to address associated threats.

Levels of deployment

Filters can be deployed at various levels throughout the information technology and communications infrastructure, *i.e.* at *i)* network level (*e.g.* Internet Service Provider network or local area networks); *ii)* server-level (*e.g.* social network site or search engine); and *iii)* end-user terminal level (*e.g.* mobile phone or computer).

Network-level filtering is deemed more effective in blocking access to pre-defined content for all users of a network. It can happen at the Internet service or access provider's network level or at the user's local area network level (*e.g.* in a school or library).

Network-level filtering's scope and objectives depend on where the filtering takes place. Filters deployed at the Internet service providers' networks are often used to filter all Internet traffic with the aim to block foremost illegal content according to local laws. Some Internet access providers offer network-based parental controls which can be activated on request of the customer to filter harmful content, block certain applications, protocols and services. Parental control for mobile Internet is usually network-based, which means that it can be either activated automatically when the mobile network operator is aware that the user is a minor or upon parents' request.[158] In local networks and closed user groups, such as a school or a library information technology system, filters operate on behalf of all connected users and enforce technical policies where certain online content and Internet services are restricted.

Content filtering is also practiced at *server level*. For example search engines operating portals in Germany and France block listings of neo-Nazi websites. In addition, "*safe search" options* are provided by major search engines and "moderate filtering", which suppresses explicit images and videos, is generally the default setting. However, "safe search" preferences can be changed by users to reduce or disable filtering. Another server-level type of filtering, more of a whitelist approach, are child versions of a portal that can be developed by service providers. Such as Junior Naver, the child version of the most popular Korean search engine which functions in a mode similar to a child safe zone.

End-user level filtering takes place on the end-user equipment through dedicated software or plug-ins to browsers or other extensions. An example for a filtering browser extension is Glubble,[159] which locks the browser (*i.e.* Firefox) so that a password is required before a user can access the Internet. Parents can then establish a user account for their child that allows them access only to a set of prescreened, child-friendly websites.

Effectiveness

Filter technology is a very efficient means in blocking blacklisted websites and has developed significantly in the past years.[160] Filtering tools are suitable against content-related risks and less effective

in reducing other online risks for children. Their effectiveness depends on percentages of false negatives and false positives, *i.e.* the rate of underblocking (allowing undesired content which should be blocked) and the rate of overblocking (not allowing content which is "good" for children).[161] Comparisons of filtering tools' effectiveness across time have shown that there has been improvement in the detection of undesired content, *i.e.* less underblocking, but less improvement in unduly blocking harmless content.[162]

The circumvention potential is another aspect to be taken into account when appraising the effectiveness of filtering solutions. For example, tests show that terminal-level filters seem to be easier to circumvent for more tech-savvy young users. For instance, filtering or blocking tools on the home computer may be circumvented by gaining control of the administrator's account (user name and password), or by using a "boot disk". Other circumvention methods known to young users include Web anonymizers, translation software, search engine caching, etc.[163]

For filters, it is particularly challenging to address dynamic content posted on peer-to-peer applications and Web 2.0 platforms.[164] Currently, risks for children are addressed by site-specific measures, and in some cases by content rating by the users community.[165] Peer-rating and community-based filtering where dynamic content is also dynamically scored is predicted as vast potential because it can react quickly to new problematic content by involving users themselves.[166] Such an example is the new "POWDER" mechanism of ICRA labeling system which directly involve end-users and enables swift classification through crowd-sourcing.

Word filters and text analysis tools have shortcomings which hamper their effectiveness and at present the technologies still produce too many false negatives and false positives in order to be reliable,[167] but it can nevertheless be put to good use as a complement to a broader security scheme, for example for prevention strategies on social communities.

Parental control software

Parental control software is the most widely used technological solution for enhancing child safety online. Based essentially on filtering technology, it includes *i)* services that require an installation or pre-installation on the end-user's hardware; *ii)* service operated only on the server or network side; *iii)* a mix of both. From a commercial perspective, server- or network-side solutions are sometimes based on a subscription model. Client-side solutions can also be subscription based, in particular where blacklists have to be maintained.

End-user level filtering software provides the maximum degree of control to parents and some network-level filtering solutions are configurable, for example by selecting categories of contents that the software should block.

Parental control software tools may perform not only content filtering, but also control of the use of certain applications (*e.g.* webcams, instant messengers), provide detailed reports on children's online usage or enable time restrictions of Internet usage. Thus, parental control software may target a wider scope of risks, beyond content-related risks, such as communication risks and over-consumption.

Recent US research emphasises that the market offers a wide selection of parental control solutions.[168] Off-the-shelf software tools for parental control are either directly purchased by parents or are provided by Internet Service Providers, with or without additional cost for the user.

Commentators point out that one of the most significant advantages of parental control solutions is that they are able to operate independently and without permission from content producers or network service providers.[169] Following this opinion, parental control software empowers families to decide what content to allow, when to allow access or what types of activities to enable on the basis of their values,

children's age and needs. According to surveys made in the US, parental control tools are deemed "effective" and the users of those tools "are generally pleased with their performance".[170] Potential disadvantages of parental control solutions discussed are their impact on the children's rights to privacy and to freely seek and receive information as part of the right to freedom of expression.

Other technologies to protect children

In many countries industry offers *children devices,* especially mobile telephony handsets configured for children, which either have limited functionality from the outset or where certain functions such as Internet access and bluetooth are disabled. In Japan, each mobile phone company is selling children devices, which cannot access Internet websites as a default setting.

US mobile phone operators allow for parental controls, including the abilities to turn off Internet access, to filter Web content and to block unwanted text messages or phone calls, a solution that also accommodates different parental needs and children's ages.[171] It is possible to create lists of blocked phone numbers to prevent unwanted calls and text messages from being sent or received. Also, to designate trusted numbers that can always communicate with your family member, regardless of other usage controls that are set.[172] On the part of parents, there is a demand for mobile phones which provides an emergency call function and can be located for instance via the Internet.

In Australia all mobile carriage service providers have implemented access control systems for mobile phones which restricts access to age inappropriate content (*i.e*. content classified MA15+ and R18+) to premium SMS and MMS numbers and in addition must be able to offer their customers the option of barring all premium SMS and MMS services in order to allow parents to prevent their children from using up their prepaid mobile phone credits or incurring large bills for a post paid mobile phone for mobile premium services.[173]

Age verification system in the online environment is used to restrict access to classified content or as an authentication mechanism. Methods currently used to verify the age of a user vary and can involve credit cards, national ID cards and even face-to-face verification. Reliance on credit cards to establish minimum age is the most widely deployed mechanism and has been criticised for its many circumvention possibilities, such as using parent's credit cards or new forms of pre-paid credit cards.[174] Face-to-face verification is another commonly used age verification method for example in Germany and the United Kingdom, however, it resorts to offline age verification. In Korea, the Identity Verification System uses the Resident Registration Number to verify the age but a recent technical framework implemented by the government, the *i*-Pin system, prevents the overexposure of this sensitive number (OECD, 2010a).

Age verification in social networking sites is a challenge which some social networks try to address using peer verification. Facebook, for instance, uses peer age verification only for users who have identified themselves as bellow 18; MySpace has a closed school section which operates on peer approval and moderation in order to divide current students from alumni; MySpace also provides a "report abuse" option which enables current users to report underage users.[175]

In Belgium, "*www.saferchat.be*" was a project funded by the EU under the STORK programme for an interoperable European eID Interoperability Platform where only children were admitted in designated chats. It was given up in 2008 due to various problems in particular its reliance on the Belgian electronic national identity card and also simply because it was not popular with the children.[176]

Technology-driven *content rating and labelling schemes* are used to enable and to some extent automate classification schemes, which in turn provide the essential input for filtering software's

interpretation of what is to be blocked.[177] For example the ICRA labels use the Resource Description Framework (RDF)[178] where the content is tagged and can be read out by common parental control systems.

> "Classification, rating and labelling are three distinct, but integrated steps, in the process of categorising content according to its suitability for minors."[179] "Classification" refers to the general process of categorising content; "rating" describes the evaluation of a single piece of content, while "labelling" is the placing of a visible mark to signal the type of content.[180]

The content labelling may originate from different sources: *i)* content producers may place labels on their own content (*e.g.* **ICRA labels** whereby content providers label their own Web content based on a questionnaire); *ii)* the rating of content may be carried out by public or private bodies (*e.g.* regulators, governmental departments, industry associations, NGOs, groups of interests,); *iii)* rating may be carried out at user community level (*e.g.* in Web 2.0 platforms).

Content rating and classification often operate at national level (*e.g.* The Australian National Classification Scheme; the cross media classification system Kijkwijzer in the Netherlands). Industry self-labelling such as the RTA-label potentially operates internationally. Pan-European rating of computer games takes place through the Pan European Game Information (PEGI) system.

The EU funded Quatro+ project aims to empower users by promoting a labelling culture. The project has developed a technological platform for delivery and authentication of machine-readable content quality labels.[181] The labels are interoperable and do not necessarily require a complete harmonisation of the rating and classification schemes used by labelling authorities in the EU. The platform allows end users to agree or disagree with the labels and also enables end users to create labels themselves.[182]

A relatively simple measure to enhance online safety which has been deployed in a number of countries is the *"report abuse" mechanisms* (also known as "panic button") on instant messaging applications and social networking sites.[183] Certain social network sites for example have implemented a technology-driven mechanism whereby users can report abuse to the site's operators dedicated staff, and young users can complain about content or conduct encountered online.[184]

Such buttons are sometimes linked to "Internet hotlines" where users can report illegal content. Providers are sometimes not aware of such reports and of the illegal content, a situation which can delay swift action to take illegal content down. Internet hotlines have a very specific remit which is to receive information abuse child sexual abuse images and combat such illegal material. Another example is Hector's World Safety button from New Zealand which helps the child cover whatever is on the screen and urges them to get an adult to help.[185]

Government policies on technical measures

Governments' approaches with respect to technical measures to protect children online vary. This section describes countries' strategies to promote the adoption of voluntary technical controls, legal obligations requiring the implementation of certain technology for the protection of children online, and public funding of research and development in such technologies.

Promotion of voluntary technical controls

In some countries, ISP-level filtering in most instances with the objective to block child sexual abuse images is implemented on the basis of self- and co-regulatory agreements (*e.g.* Canada, Denmark, New

Zealand, Norway, Sweden, and the United Kingdom). In New Zealand the Department of Internal Affairs (DIA) is offering Internet Service Providers, for use on a voluntary basis, a Digital Child Exploitation Filtering System that blocks websites identified as hosting child sexual abuse images.[186]

The Japanese "Action plan for encouraging dissemination of filtering service" promotes the improvement of filtering service availability.[187] In addition, Japanese mobile operators undertook self-regulatory efforts following up on the Minister's request to introduce blacklist filtering and offer more customizable settings for minors.[188]

The United Kingdom Child Safety Online Kitemark scheme is an effort to build trust in filtering tools and other technical solutions for home use.[189] Under this scheme, filtering products on the market are independently tested by the British Standards Institution to assess whether they provide simple and effective means of support to parents.

In 2008 Spain introduced a legal obligation for Internet service providers to inform users about *i)* both technical means and potential security risks; *ii)* available filtering tools and access management software; and *iii)* about their responsibility when using the Internet for illegal purposes.[190]

Mandating pre-installed filtering services

Other countries oblige service providers not only to provide information, but to directly provide filtering services. In Japan, mobile phone operators have to provide users under 18 with filtering services except when parents' opt-out of the services.[191] Other ISPs have to supply filtering services upon request (opt-in). Computer manufacturers are required to make filtering services available in advance.[192]

Mandatory filtering schemes

Countries which require mandatory network-based filtering from ISPs include Korea, Italy and Turkey, where illegal content is filtered according to the national laws.

The Turkish Law No. 5651 (2007) regulates the responsibility and the obligations of content, hosting and access providers, including operators of public Internet access points. For instance, cyber cafes should use filtering products approved by the Internet Regulations Department, an agency which also maintains a blacklist of sites known to host illegal and harmful content.[193]

Australia announced in late 2009 a plan to amend the Broadcasting Services Act to require ISPs to filter content rated Refused Classification (RC) and hosted in foreign jurisdictions.[194] The decision followed a live pilot of ISP-level filtering, conducted by the Australian Government and with participation of several ISPs, which showed that "ISP level-filtering of a defined list of URLs can be delivered with 100% accuracy" (*i.e.* blacklist) and that this is done "with negligible impact on Internet speed".[195]

Public funding of research

Public funds can support research on technologies to protect children online, especially where market based research and development is difficult to achieve, for example in the case of interoperability across technologies. The EU's Safer Internet Programme has been funding research into technologies, such as earlier mentioned Quatro+ and Safer Chat.[196] The Japanese Ministry of Internal Affairs and Communication supports private sector efforts to develop technology to enable the semantic analysis of messages containing illegal and harmful information.[197] Also the Australian government announced the set-up of a grants programme to encourage ISPs to offer additional filtering services on a commercial and optional basis to its end users.[198]

Conclusion

A whole toolkit of technical measures supporting the protection of children online is available. Yet there is no single technology which would resolve completely the problematic of content- and conduct-related risks for children and without unintended side effects. Most national policies include technologies in their set of measures to protect children online. The main policy making challenge is to balance the role of technologies to protect children and their impact on the risks and opportunities for children and on the wider user community, in particular where these measures restrict communications freedoms such as the right to freely receive and impart information and the right to privacy of communications.

Countries either promote voluntary take-up at various levels or, less often, mandate deployment, notably in the case of ISP-level filtering of illegal content. In some countries such as the United States and Canada, mandatory filtering is not compatible with constitutional rights related to free speech. Moreover, most countries promote the adoption of voluntary filtering schemes at the ISP-level and/or in the form of parental controls installed or activated by the users, to filter child inappropriate content and some contact-risks. The utility and scope of application of some technologies such as technology driven content-rating and age verification systems would benefit from interoperability to help unleash the functions from a given platform and operate across various infrastructures and devices.

Awareness raising and educational measures

Many awareness raising and educational initiatives to protect children online are implemented in most countries with the aim to empower children, parents and other relevant groups. A large variety of means are used to reach out and convey messages to selected populations such as children, educators and parents. They include, for example, outreach programmes, websites, online games and other interactive tools, brochures, press, radio and TV ads.

Types of awareness raising campaigns

Topical campaigns are launched with the aim to inform and educate about an issue of public concern. For example, the Netherlands ran a cybersecurity campaign throughout the summer 2009. Conversely, many awareness raising efforts take a comprehensive approach when they provide an inventory of risks children face online and advise on risk mitigation strategies. Awareness raising initiatives also promote active risk mitigation and coping strategies such as telling a trusted person, the use of reporting tools and the availability of counseling. In the United Kingdom, a large scale campaign around the slogan "Zip it, Block it, Flag it" encourages children in addition to cybersafety strategies to report any inappropriate behaviour to somebody they trust.[199]

Awareness material is tailored to suit specific audiences and communication strategies have to take into account children's development. For example, the ITU Child Online Protection (COP) Initiative includes guidelines for *i)* children; *ii)* parents, guardians and educators; *iii)* industry; and *iv)* policy makers.[200] Many awareness raising websites provide information for different types of visitors. Australia's Cybersmart website (*www.cybersmart.gov.au*), New Zealand's website NetSafe (*http://netsafe.org.nz*) and the British website ThinkUKnow (*www.thinkuknow.co.uk*) contain sections for children of different ages, parents, educators and the business community. In Australia, ACMA delivers free general awareness presentations for parents, students and teachers.[201] In the United States, the Federal Trade Commission has considerable consumer education materials designed to raise awareness among children and parents and their teachers of the types of issues that children should be aware of in the online environment.[202]

It is important that awareness material and safety tools are made available in local languages. For example, the Family Safety tool kit produced by the European awareness network (INSAFE) has been

translated to Arabic and adapted to the local context.[203] Another good practice example from the private sector is Microsoft's "Protect" sites (*www.microsoft.com/protect/default.aspx*) which have been localised into 35 languages, and the content of which is made freely available for syndication. However, there are sizeable differences among countries when it comes to the availability of quality awareness material and tools.

Offline activities such as workshops, events and presentations are as important as online awareness raising for reaching out to the target groups. One major event is the *Safer Internet Day,* organised each year in February in a growing number of countries with the aim to raise public awareness about the issue of children's safe Internet use. INSAFE, the European network of awareness centres, organises and co-ordinates local events, and participation is open to organisations from third countries. The motto for 2010 was "Think B4 U post!", highlighting the problematic aspects of children uploading information with regards to information privacy and security.[204] Other dissemination strategies involve training multipliers. In Egypt, youth ambassadors from youth Internet safety focus group ("net-aman") relay Internet ethics and etiquette to peers.

Various organisations contribute to awareness raising and educational initiatives, including *i)* public bodies; *ii)* not-for-profits organisations such as child welfare organisations and consumer associations; *iii)* businesses[205] and *iv)* public-private partnerships. Among OECD members, the prevailing types of organisation to run awareness campaigns are not-for-profits, which are often composed of multiple stakeholders, and public bodies. Some countries support NGOs management of multi-stakeholder input into policy and online safety education development, as with the New Zealand Government's relationship with non-profit NetSafe, dating back to 1998. Industry accounts for many awareness raising websites and initiatives, in particular in the context of a specific service, but rarely caters for initiatives which train critical abilities of children to engage more generally with Internet content.

The funding of awareness campaigns depends on the type of implementing body: public bodies receive public funding, not-for-profits attract funding through grants or charity, and for-profit companies may invest under the umbrella of corporate social responsibility. EU member states tend to be structurally similar due to conditions accompanying funding from the Safer Internet Programme (SIP).

Industry has an important role to educate consumers about available technical solutions to exercise parental control in relation to the offered services. In order to make this information more accessible for parents, US leading wireless carriers agreed to present relevant information under the common search term "parental controls".[206]As part of their *corporate social responsibility,* companies contribute to educational measures and support awareness raising efforts. In Poland, the Office of Electronic Communications encourages such awareness raising and educational efforts by issuing a certificate (*i.e.* "Safe Internet", "Safe phone") to communications service providers which comply with a set of conditions intended to protect children and young users.[207]

Internet literacy education

An increasing number of countries include *Internet literacy* in school curricula and organise trainings for teachers and educators. According to a recent European survey, Internet safety has been recently included in the majority of European countries.[208] Where Internet literacy education is part of the school curricula, a more recent trend is to start with Internet literacy education in elementary school, for example in Japan the appropriate use of the Internet is taught as of 2009 in elementary school as well as in Norway, and as of 2011 in the United Kingdom. In some US states, Internet safety courses are part of the required curriculum and new federal rules require schools that receive federal funding to educate minors about appropriate online behavior.[209] Egypt is testing a curriculum on digital literacy and Internet safety in secondary schools.[210] In 2009, the Australian Government provided an additional AUD 16.6 million to the

Australian Communications and Media Authority (ACMA) to continue and expand their comprehensive range of Cybersmart cybersafety education activities which includes a national outreach training programme delivering cybersafety presentations to students, parents and teachers as well as accredited professional development workshops for teachers and trainee teachers. In addition, the Australian government provided a further AUD 3 million for the national pilot to increase cybersafety in schools, which was conducted by a child safety charity (the Alannah and Madeline Foundation).

The scope of Internet literacy education varies across countries and reflects to some extent the local situations and needs. Topics range from computer skills, cybersecurity and responsible use to fostering creative and critical capabilities, participation and active citizenship.[211] Digital citizenship is a modern concept of Internet literacy which incorporates a number of elements including digital etiquette, digital literacy and digital security and which emphasizes participatory and creative opportunities of the Internet for children.[212] An additional ramification for successful Internet literacy education which is gaining importance is the enhancement of children's capacity to cope with risks and the communication of coping strategies. This modern notion of Internet literacy is only adopted by very few countries so far (*e.g.* Australia and New Zealand) and not yet fully operational even in countries where some initiatives subscribe to it.

In order to prepare schoolteachers and other trainers, almost all countries where Internet literacy is included in their school curricula offer some form of teachers' training. Australian teachers, for example, can, under the ACMA's Cybersmart programme, take an accredited Cybersafety course and a programme for trainee teachers in primary, secondary and graduate diploma teaching courses intended to build competency in Cybersafety was launched in June 2010. The ACMA's training programme will be also offered as an interactive e-learning programme in early 2011 to allow greater flexibility for teachers and schools to access cybersafety information.

In New Zealand, the NetSafe Kit for Schools (under review) offers educational materials for schools, and a separate kit has materials for the early childhood education sector.

In some cases official reviews monitor the effectiveness of this Internet literacy education for example in Australia,[213] United Kingdom and in New Zealand.

Positive content provision

The Council of Europe and many countries recognise the provision of *positive online content* as a way to *i)* offer child suitable content, *ii)* promote a beneficial online experience and *iii)* create child safe zones on the Internet.[214] Services aiming to provide positive online content for children are websites made for a child audience and Web portals, such as children's search engines and walled gardens from where children can access collections of suitable content. Standards on what is positive online content for children exist, if at all, for specific services only and those are often not systematically evaluated. The characteristics of positive online content for children vary and include for example age appropriate, diverse, affirmative, educative, participatory and/ or interactive content;[215] however, not every website which is targeted at children automatically provides positive online content.

As an instrument of public policy, positive online content for children can supplement a strategy to mitigate the risks children encounter online. Directing children towards dedicated websites protects them from the online risks, creates opportunities for children and can empower them in terms of learning, participation, creativity, and identity.[216] The EU and many countries are funding directly or indirectly the creation of positive online content for children.[217] Germany opened an annual EUR 1.5 million enveloppe which is allocated over a period of three years to provide financial support for high-quality and innovative

Internet content for children.[218] Other, in particular smaller, countries promote local online content also directed at a child audience with a view to promote online services reflecting local culture and language.

Different stakeholders are engaged in the provision of online content for children, for example publicly funded content providers such as public service media alongside many child interest initiatives and companies which maintain children's websites. As part of their remit, public service broadcasters in Europe and in the United States take the creation of children's content forward and some have created substantial portals for children.[219] On the one hand, private sector is often better equipped to set up high-end websites for children with an attractive combination of content, interactive features and free downloads. On the other hand, websites targeting children often have a commercial purpose and can thus incorporate various online marketing techniques, which can – depending on the understanding - be contrary to the notion of positive online content for children.

Even on a national basis, the volume of available online content for children can be difficult to assess given the many small and idealist initiatives. However the lack of collaboration can also translate into a downside for the take-up by children. The success of online portals for children depends on the availability of attractive and positive content for children. For example, "Kids.us" - a dedicated domain for children - was launched in 2002 in the United States as a safe space for children under 13 on the Internet and is not yet sustainable because the domain is not sufficiently populated.[220]

International co-operation

As the Internet is an open medium where information freely flows across borders, many risks faced by minors online have an international dimension. As a consequence, cross-border co-operation for the protection of children online is an important component of government policies. Bilateral co-operation and cross-border law enforcement, which are not in the scope of this study, are also key in this area. Regional policy frameworks, already addressed earlier in this report are not addressed in this section.

The protection of children online is on the international policy agenda and part of the work programme of several intergovernmental organisations and international non-governmental organisations. International co-operation takes place at policy and operational levels. Collaboration at the international policy level needs to be inclusive in order to reflect the various roles of stakeholders.

International co-operation at policy level

Insofar as online content qualifies as mass media, the UN Convention on the Rights of the Child requires that signatories encourage appropriate guidelines for the protection of the child from information and material injurious to his or her well-being, while recognising the children's fundamental right to freedom of expression and parents' primary responsibilities.[221]

ITU's Child Online Protection (COP) Initiative links an international collaborative network aiming to promote the online protection of children worldwide. The COP initiative has produced awareness material tailored to different audiences[222] and has emerged as an international platform for dialogue between governments and other stakeholders.[223] In the framework of the Internet Governance Forum (IGF), the Dynamic Coalition for Child Online Safety is an open platform for discussion carrying forward the Tunis Commitment on the role of ICTs in the protection of children and in enhancing the development of children.[224] Collaborators are child protection organisations working towards a safer Internet for children.

The International Conference of Data Protection and Privacy Commissioners in its resolution on Children's Online Privacy of 2008 supports the development of education-based approaches to improving online privacy for children and calls on operators for websites created for children to demonstrate social responsibility by adopting adequate privacy policies.[225]

Other important stakeholders for international co-operation at policy level are child welfare organisations such as Childnet International, the European Child Safety Online NGO Network (ENASCO) and the Family Online Safety Institute (FOSI) together with many locally and nationally active organisations.

Operational level

Networks of national initiatives (*e.g.* Internet hotlines, awareness centres) which collect reports of illegal online activities, have emerged as a model of organisation for operational international co-operation. Examples are INHOPE, the International Association of Internet Hotlines, INSAFE, the European network of Awareness Centres, and less visible INACH, the International Network Against Cyberhate. Another important private initiative is the Family Online Safety Institute (FOSI) which operates the ICRA content labelling framework. Some of these organisations are active stakeholders at the international policy level.

INHOPE has become truly international with thirty five members worldwide, including members from Europe, Asia, North America and Australia. The association facilitates international exchange and co-ordination of national hotlines enabling swift and effective response to reported illegal content online. To this end, INHOPE sets out policies and best practice standards for the effective operation of Internet hotlines, it promotes the establishment of new Internet hotlines and engages in public awareness raising about the illegal content online and the reporting tool. Through INHOPE, members can exchange reports about illegal material when the content is hosted abroad and take action by informing law enforcement agencies and the Internet Service Providers for removal.

The INSAFE co-operation network and its partners are working towards the safe and responsible use of the Internet and mobile devices by citizens, in particular children and youths. Through this network, INSAFE partners share best practice, information and resources, monitor and address emerging trends, reach out with Internet safety-awareness campaigns and promote Internet literacy. INSAFE is the central organiser of the Safer Internet Day which is gaining more international momentum each year. In many countries the national awareness centres have become instrumental to the national co-ordination of stakeholders for the protection of children online and the European network helps to increase the professionalism and feeds back into national policy.

The two existing international networks of national hotlines (INHOPE) and awareness centers (INSAFE) can be considered as models for successful international co-operation at the operational level.

ANNEX II – TABLES AND FIGURES

Table 4. Europe: Does your child use a mobile phone of his/her own?

Age of the child	Yes, a mobile with no access to the Internet	**Yes, a mobile with access to the Internet**	Yes, but I am not sure if it has Internet access option	**Total** Yes	**Total** No
6	9%	**1%**	1%	11%	89%
7	11%	**2%**	0%	13%	87%
8	18%	**3%**	1%	22%	78%
9	27%	**4%**	1%	32%	68%
10	45%	**6%**	1%	52%	47%
11	54%	**8%**	2%	64%	36%
12	64%	**15%**	3%	82%	18%
13	72%	**11%**	4%	87%	13%
14	67%	**17%**	3%	87%	13%
15	68%	**18%**	4%	90%	8%
16	71%	**18%**	6%	95%	5%
17	73%	**19%**	3%	95%	4%

Base: all respondents %, DK/NA not shown

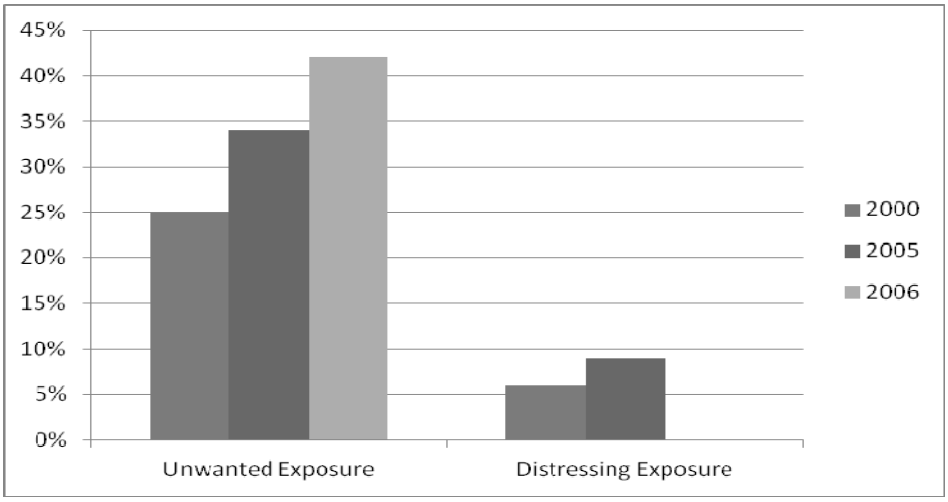
Source: EC, 2008c, p.20.

Box 2. Change in Unwanted Exposure to Sexual Material

In 2005, a study found that of 12-14 year-olds exposed to nudity, 63% are exposed through TV, 46% movies and 35% on the Internet. Another study described that younger children report encountering pornographic content offline more frequently than online (10.8% versus 8.1%). 4.5% of younger Internet users reported both online and offline exposure, 3.6% reported online-only, and 7.2% offline-only exposure in the past year. This suggests that concerns regarding large groups of young children being exposed to online pornography might be overstated.

Source : ISTTF, 2008, p. 31.

Figure 14. Exposure to Sexual Material, American 10-17 year-olds



Source: Online Victimization of Youth: Five Years Later, Ybarra ML, Mitchell KJ, Finkelhor D, Wolak J (2007) p. 9

Table 5. Percentages of children online who have seen violent content in a selection of European countries

Country	Percentage	Age considered
Ireland	90%	10-20 years olds
Poland	51%	12-17 year olds
Belgium	40%	9-12 years olds
The Netherlands	39%	13-18 years olds
Denmark	35%	9-16 years olds
Iceland	35%	9-16 year olds
United Kingdom	31%	9-19 year olds
Norway	29%	9-16 year olds
Sweden	26%	9-16 year olds
Italy	up to 25%	7-11 years olds
Austria	15%	10-15 year olds
The approximate median response is 32%		

Source: Hasebrink *et al.,* 2009 in "Kids Online" Opportunities and risks for children, p. 137.

Table 6. Children being bullied/harassed/stalked in some European countries in 2008

Country	Percentage	Age considered
Poland:	52%	
Estonia	31%	6-14 years olds
Italy	21% 18%	7-11 years olds 12-19 years olds
United Kingdom	20	11-19 year olds
Ireland: or	19%	9-16 years olds
Norway:	16%	
Sweden: of	16%	9-16 year olds
Iceland	15%	9-16 year olds
Belgium:	10%	

Source: Hasebrinks, Livingstone and Haddon (2008) comparing Children's online opportunities and risks across Europe: cross-national comparisons for EU Kids Online, p.29.

Table 7. United States: Prevalence of aggressive behaviour in gaming

Question: When you play computer or console games, how often do you see or hear people being hateful, racist or sexist while playing?	% of teens who witness behaviour (n=1064)
Often	16%
Sometimes	33%
Never	51%

Source: Pew Internet and American life project, gaming and civic engagement survey of teens/parents, Nov 2007-Feb 2008. Out of teens who play games (n=1064). Margin of error is ± 3%, p31

NOTES

1. In 1999, the ICCP issued a background report on "Approaches to content on the Internet" (see OECD, 1999) which reviewed the existing legislation and practices in member countries concerning Internet content issues including illegal, harmful, and controversial content. Many aspects covered in this report are related to the protection of children online.

2. The agenda and presentations are available at: *www.oecd.org/document/17/0,3343,en_2649_34255_43301457_1_1_1_1,00.html*

3. Cf. p. 7, for a summary of the discussion. The conference helped prepare the Review of the 1999 Guidelines on Consumer Protection in the Context of Electronic Commerce. See documentation at *www.oecd.org/site/0,3407,en_21571361_43348316_1_1_1_1_1,00.html* and *www.oecd.org/document/32/0,3343,en_21571361_43348316_43384736_1_1_1_1,00.html#*

4. Germany's Interstate Treaty on the protection of minors, Art. 3 (1).

5. Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. § 6501–6506.

6. Korean response to the APEC questionnaire.

7. Online risks for children are in many instances closely related to offline activities; bullying, for example, is not confined to online media.

8. The study is conducted within the context of the global Project on Cybercrime (*www.coe.int/cybercrime*) to assess the measures taken by countries to criminalise conduct related to the sexual exploitation and sexual abuse of children, including child pornography. The study aims to:

   - Raise awareness of existing instruments that help societies build strategies against the sexual exploitation and abuse of children.

   - Promote the implementation of common standards and harmonised legislation and a framework for effective and efficient international co-operation on cybercrime, including offences related to sexual exploitation and sexual abuse of children.

   - Serve as a database for substantive law provisions on protecting children to share good practices, encourage the implementation of these treaties and facilitate technical co-operation activities.

   - Help prepare the ground for future monitoring of legislation on child protection against sexual abuse and sexual exploitation.

9. APEC and OECD received 21 responses to the questionnaire from a mix of OECD and APEC members and non-member governments: Australia, Canada, Denmark, Egypt, European Union, Finland, Germany, Hungary, Italy, Japan, Korea, Mexico, the Netherland, the Philippines, Slovakia, Spain, Sweden, Switzerland, Thailand, Turkey and the United States, *http://aimp.apec.org/Documents/2009/TEL/TEL39-SPSG-SYM/09_tel39_spsg_sym_018.pdf.*

10. The database is available at *www.lse.ac.uk/collections/EUKidsOnline/repository.htm*.

11. Japanese Statistical Survey Department, Statistics Bureau, Ministry of Internal Affairs and Communications.

12. Data provided by the Japanese Delegation to the OECD: detail: 27% of children aged 9-12, 56.3% of children aged 13-15 and 95.5% of children aged 16-18.

13. Wolak *et al.* (2006) is one example of a recurrent study.

14. In a study for the Council of Europe, O'Connell and Bryce (2006) propose the concept "Risk of Harm from Online and Related Offline Activities" (RHOOA) in order to capture the activities and various roles children and young people assume.

15. Virtual worlds are potentially risky for children as they can face several content and contact risks such as age-inappropriate content or illegal interaction. Keeping strict rules on explicit content (violent and/or sexual), limit age of registration and access is essential as new virtual worlds are being created every day and the number of players is on a constant rise: virtual worlds counted 579 million registered accounts worldwide in the 2nd quarter of 2009, representing an increase of 38.6% in only 3 months, 80% of them being children aged from 5 to 15 years old and with the number of pre-teen (3-11) users increasing the most significantly. (US FTC, 2009b)

16. Number of unique URLs indexed by Google at 25 July 2008, *http://googleblog.blogspot.com/2008/07/we-knew-web-was-big.html*.

17. See also Canadian Media Awareness Network (MNet) at *www.media-awareness.ca/english/issues/online_hate/tactic_recruit_young.cfm*.

18. *www.cybertipline.com/en_US/documents/CyberTiplineFactSheet.pdf.*

19. Whitlock *et al.* (2006) cited in Dooley *et al.* 2009 p.109: "To identify the prevalence of self-injury message boards, five Internet search engines were used: Yahoo, Google, MSN, AOL, and Gurl.com. Terms searched included *self-injury*, *self-harm*, *self-mutilation* and *cutting*".

20. See note 9.

21. A recent Dutch study concludes that talking with people of different ages and cultural backgrounds online can positively affect children's offline social competence (Valkenburg and Peter, 2008, p. 227).

22. "Research that is 'Outdated and Inadequate?' An Analysis of the Pennsylvania Child Predator Unit Arrests in Response to Attorney General", Criticism of the Berkman Task Force Report, *www.cyberbully.org/PDFs/papredator.pdf.*

23. For a survey of explicit content in virtual worlds, see US FTC, 2009b. More broadly, the survey highlights that children in virtual worlds can face several content and contact risks such as age-inappropriate content or illegal interaction. Keeping strict rules on explicit content (violent and/or sexual), limit age of registration and access is essential as new virtual worlds are being created every day and the number of players is on a constant rise: virtual worlds counted 579 million registered accounts worldwide in the 2nd quarter of 2009, representing an increase of 38.6% in only 3 months, 80% of them being children aged from 5 to 15 years old and with the number of pre-teen (3-11) users increasing the most significantly.

24. Overall, 70% of teens have a cell phone which someone else, usually a parent, pays for; 19% pay part of the costs; and 10% pay all of the costs (Pew Internet & American Life Project, 2009, p. 4).

25. The American Psychological Association (APA) says that children under the age of 7-8 have trouble perceiving advertisers' intent.

26. European Commission workshop, *cf. http://ec.europa.eu/avpolicy/reg/avms/codes_2009/index_en.htm.*

27. According to the U.S. Children's Online Privacy Protection Act (COPPA) the age threshold, beneath which parental consent must be sought, is 13 years old. In the European Union parental consent is required as long as minors are not capable to fully comprehend the situation and to make an informed choice.

28. Japanese response to the APEC questionnaire.

29. Finnish response to the APEC questionnaire.

30. Stross (2010) suggests that some categories of children may not necessarily benefit from the Internet if it diverts them from education.

31. Livingstone and Haddon (2009, p. 22) propose that children climb a "ladder of online opportunities" starting off with information-seeking, progressing to online games and communication, and advancing to interactive forms of communication and creative and civic activities.

32. Responses to the APEC questionnaire of France, Ireland, the Netherlands, Sweden and the United Kingdom (in line with the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse of 2007).

33. See Article 29 Working Party, 2008. See Children's Online Privacy Working Group, 2009.

34 . 15 U.S.C. § 6501–6506 (Pub. L. 105-277, 112 Stat. 2581-728, enacted 21 October 1998. The FTC COPPA Rule is presently under review; FTC press release of 24 March 2010, "FTC Seeks Comment on Children's Online Privacy Protections; Questions Whether Changes to Technology Warrant Changes to Agency Rule", *www.ftc.gov/opa/2010/03/coppa.shtm.*

35. See *www.mext.go.jp/b_menu/public/2004/04111001/001.pdf.*

36. The data subject is the individual whose data is collected and processed. The data controller is the party competent to decide about the content and use of personal data. See definitions in the OECD Privacy Guidelines (OECD, 1980).

37. Safer Social Networking Principles for the EU, 2009; United States: In relation to MySpace: ISTTF 2008, Appendix A: Joint Statement on Key Principles of Social Networking Safety; in relation to Facebook: *www.attorneygeneral.gov/uploadedFiles/Press/Facebook%20agreement.pdf.*

38. The UK Kitemark label indicates that an official review attests that the product provides simple and effective means of support to parents.

39. No. 2 of the Tokyo Communiqué on Safer Internet Environment for Children as agreed by participants to the ITU/ MIC Strategic Dialogue on "Safer Internet Environment for Children" on 3 June in Tokyo, Japan, (ITU, 2009b). The YPRT toolkit (YPRT, 2009) gives detailed recommendations for improvements of technologies and infrastructures which can be helpful at the operational level and to feed voluntary commitments.

40. *E.g.* consultation of children in the Byron review, children's input on awareness-raising campaigns (ACMA, 2009a, p. 25; Byron, 2010, p. 36, 42).

41. *E.g.* youth ambassadors from Egypt's youth Internet safety focus group "net-aman" (Livingston and Haddon, 2009, p. 23)..

42. Especially vulnerable children are often in a situation in which parents are unable to play the responsible role envisaged.

43. See *www.lse.ac.uk/collections/EUKidsOnline/*

44. Hector's World Limited is a social entrepreneurship venture and a registered charity. It has a partnership with government agencies (CEOP in the United Kingdom; ACMA in Australia) to reach more young children. Its target group is children aged 2-9 years and their parents and teachers; *www.hectorsworld.com.*

45. Major syntheses of available international and European research on children's use and online risks have been accomplished through research projects funded under the Australian cyber-safety plan (the so-called "ECU review") and the EU's Safer Internet Programme (EU Kids Online project). See Dooley *et al.*, 2009, and *www.lse.ac.uk/collections/EUKidsOnline/.*

    Australia's Communications and Media Authority (ACMA) has produced two widely recognised reports reviewing technical and other measures for promoting online safety (ACMA, 2008a, 2009a).

    In the United States the ISTTF, a group of Internet businesses, non-profit organisations, academics and technology companies, completed a year-long inquiry with the release of its final report on the state of research and technology (ISTTF, 2008).

46. ACMA conducted and commissioned studies on ISP-level filtering and published the results of a life-pilot test which also addresses the economic and network efficiency arguments raised against ISP-level filtering (IIA, 2008; ACMA, 2008a and 2008b).

    Parental control technologies are investigated in three successive European studies testing products and services to voluntarily filter Internet content for children (the Deloitte SIP-Bench studies) (Deloitte Enterprise Risk Services, 2008).

    The Technology Advisory Board of the ISTTF reviewed the state of the art of various technologies which could be deployed in order to protect children online, including identity authentification, age verification, text-analysis filtering and monitoring technologies (ISTTF, 2008, p. 39 f.).

47. The European Commission sought the views of stakeholders and collected feedback on the following topics: Child safety and mobile phone services in 2006; online technologies for children in 2007; and age verification, cross media rating and social networking in 2008. The consultation documents are used as background information for discussion and help to better target the action areas of the Safer Internet Programme. All consultations, submissions and results are accessible through the European Commission Portal at *http://ec.europa.eu/information_society/activities/sip/policy/consultations/index_en.htm.*

    In 2009, the US Federal Communications Commission (FCC) conducted consultations on parental control technologies for video or audio programming and submitted a final report to the Congress (US FCC Report, 2009). Stakeholders were also invited to contribute to the public inquiry of the ISTTF which reviewed 40 submitted technologies for their potential to mitigate online risks for children. Hence, public consultations can feed into the policy making process and are the most inclusive means to collect input from stakeholders and the interested public.

48. Independent experts carried out programme evaluations of the previous Safer Internet Programme and its predecessors. The evaluation methodology is based on performance indicator criteria, which are used to assess the programme's cost-effectiveness and whether its objectives are met. Indicators include: quantitative/qualitative data on reporting points; the degree of awareness of EU citizens about reporting points, harmful conduct online, and empowerment issues; the number of children involved; and other outputs. European Comission Staff Working Document SEC(2008) 242, Accompanying document – Impact Assessment, Brussels, 27.2.2008, p. 8, 45f, 53.

    The proposal for the current funding programme examined the economic impact of different policy options according to four criteria: *i*) deployment and use of ICT; *ii)* cost of medical and psychological treatment*; iii)* cost to public administration, and *iv)* economic impact on third countries (EC, 2009b) Accompanying

measures such as benchmarking, testing of regulatory and technical tools, opinion surveys and studies can also be useful for programme evaluations.

49. The evaluation concept lays down specific indicators (and how to collect the data), gives current values and formulates targets (decrease or increase). For example, it refers to a study by the Office of Communications (Ofcom) in which 18% of UK children in 2009 said they had come across harmful or inappropriate content. The aim is to decrease this figure which will be evaluated one year after. In addition, the Council for Child Internet Safety's activities will be subject to an independent review (UKCCIS, 2009).

50. Its first strategy was published at the end of 2009 (UKCCIS, 2009); see also OSTWG, 2010, p. 10.

51. Powell *et al.* (2010, p. 3 f.) point out the dangers stemming from a moral panic framework dominated by concerns over sexual content and solicitation.

52. See for example the Eurobarometer surveys conducted under the Safer Internet Programme.

53. *www.itu.int/council/groups/wg-cop/.*

54. APEC and OECD have received 21 responses to the questionnaire from a mix of OECD and APEC members and non-member governments: Australia, Canada, Denmark, Egypt, European Union, Finland, Germany, Hungary, Italy, Japan, Korea, Mexico, Netherland, Philippines, Slovakia, Spain, Sweden, Switzerland, Thailand, Turkey and the United States. Available at *http://aimp.apec.org/Documents/2009/TEL/TEL39-SPSG-SYM/09_tel39_spsg_sym_018.pdf*

55. Council of Europe, Recommendation Rec (2006)12 of the Committee of Ministers to member states on empowering children in the new information and communications environment (Adopted by the Committee of Ministers on 27 September 2006 at the 974th meeting of the Ministers' Deputies).

56. Council of Europe, (2009).

57. There is presently no national legislation pursuant to Council of Europe's Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children on the Internet (Adopted by the Committee of Ministers on 20 February 2008 at the 1018th meeting of the Ministers' Deputies).

58. European Parliament and Council, 2007.

59. European Parliament and Council, 2006. See also Article 16 paragraph 1 e) of the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').

60. EC, 2009a, p. 1.

61. See *http://ec.europa.eu/information_society/activities/sip/policy/programme/index_en.htm and SIP Factsheet: http://ec.europa.eu/information_society/doc/factsheets/018-safer-internet.pdf*

62. Government of Canada, 2000, p. 5. Horton, M., and Thomson, J. (2008). "Chapter V: Canada", in FOSI, 2007, p. 61.

63. US response to the APEC questionnaire. In the US, under 2008 legislation, the Protecting Children in the 21st Century Act (Title II of the Broadband Data Services Improvement Act, codified as Public Law No: 110-385 (10 October 2008)), the National Telecommunications and Information Administration (an agency within the U.S. Department of Commerce), established the Online Safety and Technology Working Group (OSTWG) to examine industry efforts to promote a safe online environment for children. The OSTWG is comprised of 30 non-federal members and representatives from the FTC, Federal Communications Commission, Department of Justice and Department of Education. In its June 2010 report to NTIA and Congress, the OSTWG addressed four areas: 1) educational efforts, filtering controls, and labels; 2)

industry efforts to report online child pornography; 3) record retention in connection with crimes against children; and 4) protection technologies. The report contained numerous recommendations, including promoting digital citizenship in pre-K-12 education as a national priority, getting young people involved in risk-prevention education, engaging in awareness building efforts about protective technologies and promoting transparency for parents as to what sort of content and information will be accessible to their children while using a given product.

64. US Children's Online Privacy Protection Act (COPPA) and corresponding Rule.

65. US CAN-SPAM Act, 15 USC §§ 7701-7713, FTC's Adult Labeling Rule, 16 CFR Part 3164, strive to place a bumper between x-rated email and children, see *www.ftc.gov/bcp/bcpmp.shtm*; 2003 Truth in Domains Name Act, 18 U.S.C. § 2252B (2008).

66. Byron, T., 2008.

67. UKCCIS, 2009.

68. UKCCIS members committed to update three sets of guidance in 2010:

- guidance for organisations that moderate interactive services;
- guidance for providers of chat, instant messaging and other web-based services; and
- guidance for search providers on how they can help parents make sure that children and young people can search without finding things that are not suitable for them.

69. OECD, 2009a, p. 1.

70. Japan: Act on Development of an Environment that Provides Safe and Secure Internet Use for Young People of 2008, pursuant to which Web sites encouraging to commit a crime or breach the law or include information that directly and expressly induces a suicide, obscene content and extremely cruel descriptions are regulated.

Korea: Act on Promotion of Information and Communications Network Utilization and Information Protection of 2007, which regulates restricted access and advertising of content harmful to minors, requires companies to dedicate personnel in charge of juvenile protection and also introduced the requirement of an identity verification system for bulletin boards, portals and online communities of a certain size.

Turkey: Law No. 5651 (2007) prohibiting, in addition to obscene material, Web sites which amonth other things would ease drug use, supply drugs, provoke suicide as well as operate online gambling. The law can be enforced against content providers and Internet intermediaries when they are in the position to suppress prohibited content and services. The objectives of this law make reference to an article in the Turkish constitution providing for the protection of the peace and welfare of the family and especially children. See also see Akdeniz, Yaman (2010).

71. Pursuant to the 2003 Truth in Domains Name Act, 18 U.S.C. § 2252B (2008). the use of misleading domain names, words, or digital images on the Internet with intent to deceive a person into viewing obscenity is forbidden and can be sanctioned. Sanctions are higher where this behaviour attempts to deceive a minor into viewing material that is harmful to minors on the Internet.

72. Law n°2007-297, 5 March 2007, art. 44 JORF 7 March 2007. Penal Code, Article 222-33-3: The deliberate recording or photographing and the diffusion of certain violent assaults, except when carried out to serve as proof in a court or by professionals to inform the public, can lead to a maximum of 5 year imprisonment and EUR 75 000 fine.

73. See note 9.

74. *http://ec.europa.eu/avpolicy/reg/tvwf/protection/index_en.htm.*

75. Australia: Schedule 7 to the Broadcasting Act 1992. Germany: KJM, 2009. New Zealand: Department of Internal Affairs (n.d.).

76. See Germany's response to the APEC questionnaire. This gap in the legislative responses to content-related risks for children appears to be present in all countries which leaves a question mark as to whether this is justified in the light of the widespread use of these technologies by children. Individual electronic communications however is protected against censorship by the right to privacy of personal correspondence or the confidentiality of communications vested by countries' constitutions.

77. *E.g.* in Germany for adolescents from 16 years until 18 years, when they are considered adults. In Australia for example the classification MA15+ has been introduced for mobile premium services or other fee-paying services that provide audio or video content without access restriction systems.

78. Content classification is not done for every content automatically which would be regarded as a form of unconstitutional up-front censorship but official classification bodies act upon request and there is often a duty placed on the content originator to seek classification when necessary and to be transparent and accountable in their decisions. National classification schemes are challenged by the Internet, where content stemming from abroad and to which different laws apply is accessible everywhere.

79. OECD, 2009c, p. 3.

80. Pursuant to Australia's new Schedule 7 to the Broadcasting Act 1992, the Australian Communications and Media Authority (ACMA) can investigate complaints against Internet service providers, which are hosting prohibited content (*i.e.* for example adult pornography classified 'X 18+' as well as in certain circumstances content classified 'R 18+' and 'MA15+'), and administer "take down" or "access removal" notices to remove access and also the links to illegal content. In Turkey under Law No. 5651 (2007), the Telecommunications Communication Presidency (TIB) has the competence to request the take down of certain categories of online content from Internet service providers.

81. OECD, 2010b.

82. For example Swiss telecommunications providers are obliged to bar customers and users known to be under 16 from accessing value-added services with erotic or pornographic content pursuant to Swiss Ordinance of 9 March 2007 on Telecommunications Services (OTS), Art. 41.

    In Germany, the Interstate Treaty on the protection of minors mentions as possible mechanisms to ensure that children do not normally see or hear inappropriate content age verification systems, separation of adult content from content aimed at children or scheduling availability of the content, *i.e.* adhering to a "watershed" or "time window" also for online content.

    Another example for accompanying technical measures to complement (or even substitute for) content regulation is the obligation in Japan to use filtering technologies for under age mobile phone users, with an opt-out possibility left to parents. Conversely, pre-installed filtering is not required for Internet access but has to be provided upon parents' request (opt-in).

    In Australia, the *Restricted Access Systems Declaration 2007* (made under subclause 14(1) of Schedule 7 of the Broadcasting Services Act 1992*)* provides that age inappropriate content made available online, must be subject to an access control system that verifies the age of those seeking access.

83. Pursuant to the Act on Promotion of Information and Communications Network Utilization and Information Protection of 2007 mass-audience information and communications service providers in Korea have to designate personnel in charge of juvenile protection. Spanish Internet service providers have the statutory duty to inform their customers about online risks for children and available filtering technologies under Spanish Law 32/2002 on Information Society Services and Electronic Commerce.

84. The anti-indecency provisions of the US Communications Decency Act (the CDA) have been found unconstitutional in *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).

85. Canadian Criminal Code, R.S.C. 1985, c. C-46, Sec. 164.1. Horton, M., and Thomson, J. (2008). "Chapter V: Canada". In FOSI, 2007, p. 62.

86. Dooley, 2009, p. 36.

87. Responses to the APEC questionnaire of France, Ireland, United Kingdom, the Netherlands and Sweden. Art. 23 of the Council of Europe (2007). Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Lanzarote, 25 October 2007. The Convention introduces a new offence concerning the solicitation of children through information and communication technologies for sexual purposes and more countries are expected to update their criminal laws accordingly.

88. Mimi Ito in Livingstone, S., and Haddon, L, 2009, p. 33.

89. S. 431, Keeping the Internet Devoid of Sexual Predators Act of 2008, see *www.govtrack.us/congress/bill.xpd?bill=s110-431*

90. US response to the APEC questionnaire.

91. USC 47 Section 223 of title 47 as amended by the Communications Decency Act: In Australia, stalking is criminalised by legislation in each Australian State and Territory, for example the Queensland *Amendment Act 1999* (Qld).

92. See National Conference of State Legislators, Enacted Cyberbullying Legislation, available at *www.ncsl.org/Default.aspx?TabId=12903.*

93. Swedish Act (1998:112) on Responsibility for Electronic Bulletin Boards introduced mandatory monitoring of bulletin boards and messenger service for unlawful content such as child sexual abuse images and illegal description of violence by the service provider.

94. Mimi Ito in Livingstone, S., and Haddon, L., 2009, p. 33.

95. Required under the Korean Act on the Promotion of Information and Communications Network Use and Information Protection.

96. In Australia, in accordance with the Interactive Gambling Act 2001 it is an offence to provide interactive gambling services (typically online casino like games played for money) to Australians as well as to advertise such services.

97. Art. 9 (1) e) of the Audiovisual Media Services Directive 2007.

98. Art. 9 (1) g) of the Audiovisual Media Services Directive 2007.

99. See Nordic Consumer Affairs Ministers, n.d.

100. Korean Act on Promotion of Information and Communications Network Utilization and Information Protection of 2007.

101. US CAN-SPAM Act, 15 USC §§ 7701-7713, FTC's Adult Labeling Rule, 16 CFR Part 3164, see *www.ftc.gov/bcp/bcpmp.shtm.*

102. For example according to national implementations of the EU Data Protection Directive 95/46/EC which is currently under review.

103. See Article 29 Working Party (2008), p. 6 and 9.

104. Ibid.

105. US FTC (n.d.) Children's Online Privacy Protection Rule; Final Rule, 16 CFR Part 312, Federal Register: 3 November 1999 (Volume 64, Number 212), p. 59887f. The rule is presently under review, see FTC press release (US FTC, 2010).

106. In March 2010, the FTC requested public comment on its implementation of COPPA and the comment period closed on 30 June 2010. Specifically, the FTC asked for comments on the costs of benefits of the COPPA Rule (the Rule implemented pursuant to COPPA), as well as on whether it, or certain sections, should be retained, eliminated, or modified. In connection with this review, the FTC held a Roundtable on 2 June 2010 to explore some of these issues. See *www.ftc.gov/opa/2010/03/coppa.shtm* and *www.ftc.gov/bcp/workshops/coppa/index.shtml.*

107. Council of Europe Convention on Cybercrime, Budapest, 23 November 2001.

108. See YouTube Fact Sheet, available at *www.youtube.com/t/fact_sheet* (accessed 30 January 2010)

109. OECD, 2010d.

110. US FTC 2007, p. 14.

111. Children's Online Privacy Working Group, 2009.

112. Hans-Bredow-Institut and the Institute of European Media Law, 2006, p. 17.

113. See US FTC 2007, p. 22.

114. See European Framework for Safer Mobile Use by Younger Teenagers and Children, February 2007, available at *http://ec.europa.eu/information_society/activities/sip/docs/mobile_2005/europeanframework.pdf*; Safer Social Networking Principles for the European Union, 2009. Attorneys General Multi-State Working Group, In relation to MySpace: Joint Statement on Key Principle on Social Network Site Safety, available at *http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report-APPENDIX_A_Joint_Statement.pdf*; and in relation to Facebook: *www.attorneygeneral.gov/uploadedFiles/Press/Facebook%20agreement.pdf*

115. See *http://ec.europa.eu/information_society/activities/sip/self_reg/index_en.htm*

116. See overview at Jakubowicz, 2009, p. 28f.

117. European Framework for Safer Mobile Use by Younger Teenagers and Children, February 2007. Available at *http://ec.europa.eu/information_society/activities/sip/docs/mobile_2005/europeanframework.pdf*

118. PricewaterhouseCoopers, 2009.

119. Clause 3.1.16 of the Mobile Premium Services Code C637:2009 (an industry code of practice registered by the ACMA under the Telecommunications Act 1997 in accordance with co-regulatory arrangements).

120. Clause 4.4 of the Mobile Premium Services Code C637:2009.

121. In relation to MySpace: Joint Statement on Key Principle on Social Network Site Safety, available at *http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report-APPENDIX_A_Joint_Statement.pdf*; In relation to Facebook: *www.attorneygeneral.gov/uploadedFiles/Press/Facebook%20agreement.pdf*

122. In the case of MySpace, see Joint Statement on Key Principle on Social Network Site Safety, available at *http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report-APPENDIX_A_Joint_Statement.pdf.*

123. Safer Social Networking Principles for the EU, 2009.

124. See also Article 29 Working Party (2009), p. 11.

125. The "Safer Social Networking Principles for the EU" cover seven main areas:
1. awareness raising;
2. age appropriate services;
3. user empowerment through technologies;
4. easy-to-use mechanisms to report conduct or content that violates the terms of service;
5. response to notifications of illegal content or conduct;
6. enable and encourage users to employ a safe approach to personal information and privacy;
7. assess the means for reviewing illegal or prohibited content/conduct.

126. European Framework for Safer Mobile Use by Younger Teenagers and Children, February 2007.

127. Staksrud and Lobe, 2010, p. 5.

128. PEGI, n.d.

129. See also the 1999 OECD Guidelines on Consumer Protection in the Context of Electronic Commerce, which address children's protection issues in Part II, Section II, calling for special care in advertising and marketing to children online, and the 2008 OECD Policy Guidance for Addressing Emerging Consumer Protection and Empowerment Issues in Mobile Commerce ("policy guidance on mobile commerce") [DSTI/CP(2007)5/FINAL].

130. Examples for a general scheme is the ICC's Advertising and Marketing Communication Practice; specific to marketing to children are the Self-Regulatory Guidelines for Children's Advertising by CARU or the non-binding Ethical Guidelines for Advertising to Children by European Association of Communication Agencies (EACA, 2006).

131. The International Chamber of Commerce's (ICC) Advertising and Marketing Communication Practice for example contains a section on children requiring special care in marketing directed to or featuring children or young people and provides guidance on what it entails. It covers the separation of content and advertising, promotes fair information principles, the protection of certain social values with respect to , for example, marketing that appeal to children to persuade their parents or other adults to buy products for them. ICC's Advertising and Marketing Communication Practice, article 18.

The Federation of European Direct and Interactive Marketing (FEDMA) code which is relevant to direct marketing contains specific provisions for children which interpret existing data protection laws and resolves that promotional benefits should not be made conditional on the child disclosing more personal data. Federation of European Direct Marketing (FEDMA). European Code of Practice for the Use of Personal Data in Direct Marketing.

132. The Forum of Responsible Food Marketing Communication Denmark, for example, operates a voluntary code covering all platforms. Voluntary Code on advertising food in media towards children, available at *http://kodeksforfoedevarereklamer.di.dk*: Likewise, the US based Better Business Bureau operates the Children's Food and Beverage Advertising Initiative, a programme of voluntary self-regulation, see *www.bbb.org/us/children-food-beverage-advertising-initiative/*

133. *E.g.* the UK Advertising Standards Authority (ASA) now has the possibility to bring companies' marketing communications on to their own websites and other non-paid-for online space (such as social networking sites) within the remit of the Committee of Advertising Practice (CAP) code. See Byron, 2010, p. 28.

134. Article 29 Working Party, 2010, p. 17.

135. See Hans-Bredow-Institut and the Institute of European Media Law, 2006. Germany's concept of "regulated self-regulation", see also Rickert, Th. (2008). "Chapter III: Germany", in FOSI, 2007, p. 37f.

136. Rickert, Th. (2008) in FOSI, 2007, p. 37f.

137. KJM, 2009.

138. NICC, 2008.

139. Subcode of Conduct for Search Engine Providers of the Association of Voluntary Self-Regulating Multimedia Service Providers. Available at *www.fsm.de/en/Subcode_of_Conduct_for_Search_Engine_Providers.*

140. ACMA, 2008a, p. 46.

141. See OECD, 2007a.

142. Compare National Conference of State Legislators, Enacted Cyberbullying Legislation, available at *www.ncsl.org/Default.aspx?TabId=12903*

In New Zealand, the awareness center offers a NetSafe Kit for schools where model policies, procedures and use agreements can be downloaded. See NetSafe Cybersafety Kit for schools, available at *www.cybersafety.org.nz/kit/.*

143. PEGI, n.d.

144. Japanese response to the APEC questionnaire.

145. See *www.internethotline.jp/index-en.html*

146. UK Home Office, 2005, 2008.

147. See Byron, 2008, p. 74, 84; UKCCIS, 2009, p. 11.

148. US FCC, 2009, para 167.

149. Thierer, 2009a, p. 249.

150. See *www.fragfinn.de/kinderliste.html*

151. US FCC, 2009, para. 150.

152. Deloitte Enterprise Risk Services (2008), p. 14.

153. For example using the ICRA (Internet Content Rating Association) questionnaire provided by FOSI.

154. Powell *et al*, 2010, p. 8. See also the public consultation of the Australian government on measures to improve accountability and transparency of processes for the placement of material on the RC content list (closed on 12 February 2010), available at *www.dbcde.gov.au/funding_and_programs/cybersafety_plan/transparency_measures*.

155. IIA, 2008, p. 58.

156. ISTTF, 2008, APPENDIX D: Technology Advisory Board Report, p. 12f.

157. Ibid.

158. ACMA, 2009a, p. 39.

159. *www.glubble.com*

160. ACMA, 2008b, p.49f.

161. Deloitte Enterprise Risk Services, 2008, p. 28f.

162. Deloitte Enterprise Risk Services, 2008, p. 5; ACMA, 2009a, p. 32.

163. See ACMA Filtering software at *www.acma.gov.au/WEB/STANDARD/pc=PC_90167*. ACMA, 2008a, p. 44.

164. For example social networking sites or video sharing Web sites, Deloitte Enterprise Risk Services; 2008. p. 5.

165. ACMA, 2009a, p. 46; Deloitte Enterprise Risk Services, 2008, p. 13f.

166. Deloitte Enterprise Risk Services, 2008, p. 6.

167. ISTTF, 2008, APPENDIX D: Technology Advisory Board Report, p. 12.

168. US FCC, 2009, p. 62

169. US FCC, 2009, p. 57

170. US FCC, 2009, p. 63 in FN 550.

171. US FCC, 2009, p. 63.

172. US FTC, 2009a, Beyond Voice: Mapping the Mobile Marketplace, p. 32.

173 Telecommunications Service Provider (Mobile Premium Services) Determination 2010 (No.1) at *www.comlaw.gov.au/ComLaw/Legislation/LegislativeInstrument1.nsf/asmade%5Cbyid/3074416A04A9C785CA2576DF007F126F?OpenDocument*

174. ACMA, 2009a, p. 43.

175. ISTTF, 2008, p. 25

176. It aimed to establish a safer environment for chatting on the Internet through an age verification system based on the use of a Belgian electronic identity card. Under this scheme, safer chat rooms were only available to users with a child ID. EC, 2008a, p.11

177. ACMA, 2008a, p. 45.

178. Technical Standards Used, About ICRA, *www.fosi.org/icra/*

179. EC, 2008b. Background Report on Cross Media Rating and Classification, and Age Verification Solution, p.4.

180. EC, 2008b. Background Report on Cross Media Rating and Classification, and Age Verification Solution, p.4.

181. EC, 2008b. Background Report on Cross Media Rating and Classification, and Age Verification Solution, p.14

182. About Quatro Plus ND. *www.quatro-project.org/about*

183. ISTTF, 2008, p. 24; CEOP 2008: p. 21.

184. ISTTF, 2008, p. 24.

185. The Australian Cybersafety Help Button was launched in December 2010.

186. See *www.dia.govt.nz/diawebsite.nsf/wpg_URL/Services-Censorship-Compliance-Digital-Child-Exploitation-Filtering-System?OpenDocument*

187. Japanese response to the APEC questionnaire.

188. Presentation of Koji Ouchi, Deputy Director, Ministry of Internal Affairs and Communications (MIC), Japan and Koji Isozumi, Deputy Director, Minisry of Economy, Trade and Industry (METI), Japan: "Workshop on Initiatives in Promoting Safer Internet Environment for Children", APEC-OECD Joint Symposium on Initiatives among Member Economies Promoting Safer Internet Environment for Children, available at *www.oecd.org/document/17/0,3343,en_2649_34255_43301457_1_1_1_1,00.html*

189. See *www.bsigroup.com/en/ProductServices/Child-Safety-Online-Software/*

190. Spanish Law 32/2002 on Information Society Services and Electronic Commerce. Information provided in the APEC Children Protection Project Questionnaire by the Spanish respondents

191. Pursuant to the Japanese Law on environment of development for children's Internet usage.

192. Information provided in the APEC Children Protection Project Questionnaire by the Japanese respondents.

193. Information provided in the APEC Children Protection Project Questionnaire by the Turkish respondents; In this context see Akdeniz, Yaman (2010). Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship.

194. See *www.dbcde.gov.au/funding_and_programs/cybersafety_plan/internet_service_provider_isp_filteringand* Media Release of the Minister for Broadband, Communications and the Digital Economy of December 15, 2009 at *www.minister.dbcde.gov.au/media/media_releases/2009/115*

195. See *www.dbcde.gov.au/funding_and_programs/cybersafety_plan/internet_service_provider_isp_filtering/isp_filtering_live_pilot*

196. STORK project, available at *https://www.eid-stork.eu/index.php?option=com_content&task=view&id=86&Itemid=83*

197. Japanese response to the APEC Children Protection Project Questionnaire

198. Conroy, 2009.

199. See *www.dcsf.gov.uk/ukccis/news_detail.cfm?newsid=40&thisnews=2*

200. Available at *www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/index.html*

201. The presentations are tailored to the target audience including age appropriate Internet safety awareness presentations for school students aged from 9 years. The tailored presentations are designed to highlight the potential risks faced by that age group when online and provide them with tips and strategies to stay safe online See *www.cybersmart.gov.au/en/Schools/Book%20school%20seminars.aspx*

202. Most recently (December 2009), along with other U.S. government agencies, the FTC released Net Cetera: Chatting with Kids About Being Online. This booklet tells parents and teachers what they need to know to talk to kids about issues like cyberbullying, sexting, mobile phone safety, and protecting the family computer. The booklet is available at OnGuardOnline.gov, the federal government's online safety Web site.

203. Available at Cyber Peace Initiative's Web site *http://smwipm.cyberpeaceinitiative.org/page/family_kit*

204. EC (2009). Empowering and Protecting Children online, p. 2.

205. See for example *www.TeachToday.eu*

206. FTC Staff Report (2009). Beyond Voice: Mapping the Mobile Marketplace, p. 32.

207. Republic of Poland, Office of Electronic Communications, press release of 16 February 2009 "Participation in the UKE Certificate Project". Available at *www.en.uke.gov.pl/ukeen/index.jsp?news_cat_id=56&news_id=746&layout=1&page=text&place=Lead01*

208. EURYDICE (2009). Summary Report. Education on Online Safety in Schools in Europe; Staksrud, Elisabeth & Lobe, Bojana (2010). Evaluation of the Implementation of the Safer Social Networking Principles for the EU Part I: General Report.

209. US FCC Report (2009). In the Matter of Implementation of the Child Safe Viewing Act; Examination of Parental Control Technologies for Video or Audio Programming, para. 172.

210. Egypt's response to the APEC questionnaire.

211. ACMA (2009). Developments in Internet filtering technologies and other measures for promoting online safety Second annual report, p. 51.

212. ACMA (2009). Developments in Internet filtering technologies and other measures for promoting online safety Second annual report, p. 51; Livingstone, S., and Haddon, L. (2009). EU Kids Online: Final report, p. 25.

213. In Australia, the ACMA has taken steps to evaluate its awareness raising programs in the area of cybersafety education, in particular Hector's World™, which forms a key component of ACMA's cybersafety education portal, and the Cybersmart Detectives online education game. The research will examine the effectiveness of the latter game on students' cybersafety knowledge and determine if students are able to link these cybersafety messages to their own online behaviours outside the game environment. The ACMA also commissioned an independent review and evaluation of its Cybersafety Outreach Program in 2010 with results expected in the first half of 2011.

214. Council of Europe, 2009.

215. De Haan, J. and Livingstone, S. (2009) Policy and research recommendations, p. 9; Livingstone, S. (2009). "A Rationale for Positive Online Content for Children". Communication Research Trends Volume 28 (2009) No. 3, p. 12, 16f.

216. De Haan, J. and Livingstone, S. (2009) Policy and research recommendations, p. 10; Livingstone, S. (2009). "A Rationale for Positive Online Content for Children". Communication Research Trends Volume 28 (2009) No. 3, p. 12, 15f.

217. Under the EU's Safer Internet Plus Programme.

218. Germany's response to the APEC-OECD questionnaire.

219. Livingstone, S. (2009). "A Rationale for Positive Online Content for Children". Communication Research Trends Volume 28 (2009) No. 3, p. 12, 14f.

220. *www.cms.kids.us*; Web sites complying with the portal's guidelines can be self-activated and the portal operator will remove content found to breach these guidelines.

221. UN Convention on the Rights of the Child, Art. 17.

222. ITU COP Guidelines for children; parents, guardians, and educators; industry and policy makers are available from *www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/index.html*

223. Collaborating organisations are UN agencies, children rights organisations, industry associations and companies. The ITU carried out a survey of its 191 Member States on the current state of policy and provision in their countries in relation to online child safety, which will be published shortly. Findings show that there was a very low level of development of policies and laws around online child protection issues among countries classified under the UN system as "Least Developed". Among countries categorised as "Developing" the picture was more uneven, but in general there was little evidence of major activity around online child protection. Among the "Developed" nations there were higher levels of activity and a more developed legal framework. However what was striking from the survey was a more or less universal acknowledgement that each nation could benefit by being connected to information about resources and potential sources of help and assistance which would assist them domestically.

224. *www.intgovforum.org/dynamic_coalitions.php?listy=13*

225. 30th International Conference of Data Protection and Privacy Commissioners (2008).

BIBLIOGRAPHY

30th International Conference of Data Protection and Privacy Commissioners (2008), Resolution on Children's Online Privacy. Available at *www.priv.gc.ca/information/conf2008/res_cop_e.cfm*

ACMA (Australian Communications and Media Authority) (2008a), "Developments in Internet filtering technologies and other measures for promoting online safety". First annual report to the Minister for Broadband, Communications and the Digital Economy, February 2008. Available at *www.acma.gov.au/webwr/_assets/main/lib310554/developments_in_internet_filters_1streport.pdf*

ACMA (2008b), "Closed Environment Testing of ISP Level Internet Content Filtering", Report to the Minister for Broadband, Communications and the Digital Economy, June 2008, Available at: *www.acma.gov.au/webwr/_assets/main/lib310554/isp-level_internet_content_filtering_trial-report.pdf*

ACMA (2009a), "Developments in Internet filtering technologies and other measures for promoting online safety". Second annual report to the Minister for Broadband, Communications and the Digital Economy. April 2009, Available at *www.acma.gov.au/webwr/_assets/main/lib310554/developments_in_internet_filters_2ndreport.pdf*

ACMA (2009b), "Click and Connect: Young Australian's use of online social media". 02: Quantitative research report, July 2009. Available at *www.acma.gov.au/webwr/aba/about/recruitment/click_and_connect-02_quantitative_report.pdf*

Adkeniz, Y. (2010). Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship. Available at *www.osce.org/fom/41091.*

Article 29 Working Party (2008), "Working Document 1/2008 on the protection of children's personal data" (General guidelines and the special case of schools). Available at *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp147_en.pdf*

Article 29 Working Party (2009), "Opinion 5/2009 on social networking". Available at *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf*

Article 29 Working Party (2010), "Opinion 2/2010 on online behavioural advertising". Available at *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp171_en.pdf*

Australian Department of Education, Employment and Workplace Relations (2008), "Behind the scenes insights into the human dimension of covert bullying". Available at *http://pandora.nla.gov.au/pan/101323/20090617-1056/www.deewr.gov.au/Schooling/Behind.pdf*

Bartoli, E. (2009), "Children's Data Protection vs. Marketing Companies". *International Review of Law, Computers & Technology*, 23(1-2), 35-45.

Beantin Webbkommunikation (2010), "Internet usage and young Swedes in Sweden", *http://beantin.se/post/616872465/internet-use-sweden-young-swedes-children-age-group*

Branch Associates (2002), NetSmartz evalulation project: Internet safety training for children and youth ages 6 to 18. Atlanta: GA: Boys & Girls Clubs of America and National Center for Missing & Exploited Children.

British Standards Institution (BSI) (n.d), "Kitemark for Child Safety Online". Available at *www.bsigroup.com/en/ProductServices/Child-Safety-Online-Software/*

Byron, T. (2008), "Safer Children in a Digital World: The Report of the Byron Review". London: Department for Children, Schools and Families, and the Department for Culture, Media and Sport. Available at *www.dcsf.gov.uk/ukccis/userfiles/file/FinalReportBookmarked.pdf*

Byron, T. (2010), "Do we have safer children in a digital world? A review of progress since the 2008 Byron Review". March 2010. Available at *www.dcsf.gov.uk/byronreview/pdfs/do%20we%20have%20safer%20children%20in%20a%20digital%20world-WEB.pdf*

Carr, J., and Hilton, Z. (2009), "Children's Charities' Coalition on Internet Safety Digital manifesto". Available at *www.nspcc.org.uk/Inform/policyandpublicaffairs/Westminster/ChildSafetyOnline_wdf48584.pdf*

Child Exploitation and Online Protection Centre (2008), "Annual Review", December 2008, Available at *http://ceop.gov.uk/downloads/documents/ceopannualreview2008.pdf*

Child Health Promotion Research Centre, Edith Cowan University (2009), "Australian Covert Bullying Prevalence Study". Available at *www.deewr.gov.au/Schooling/NationalSafeSchools/Pages/research.aspx*

Children's Online Privacy Working Group (2009). "There ought to be a law: Protecting Children's Online Privacy in the 21st century". A discussion paper for Canadians by the Working Group of Canadian Privacy Commissioners and Child and Youth Advocacies. 19 November, 2009. Available at *www.ombudsman.yk.ca/pdf/Children'sOnlinePrivacy-e.pdf*

Connect Safely (2009), "Online Safety 3.0: Empowering and Protecting Youth". Available at *www.connectsafely.org/Commentaries-Staff/online-safety-30-empowering-and-protecting-youth.html*

Conroy, Stephen (2009), "Measures to Improve Safety of the Internet for Families", in: *Minister Speeches,* 15 December 2009. Available at *www.minister.dbcde.gov.au/media/speeches/2009/075*

Cosgrove, M. (2009), "Young French bloggers find a new and risky way to create buzz". Available at *www.digitaljournal.com/article/278496.*

Council of Europe (2006), Recommendation Rec(2006)12 of the Committee of Ministers to member states on empowering children in the new information and communications environment (Adopted by the Committee of Ministers on 27 September 2006 at the 974th meeting of the Ministers' Deputies). Available at *https://wcd.coe.int/ViewDoc.jsp?Ref=Rec(2006)12&Language=lanEnglish&Site=CM&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864*

Council of Europe (2007), "Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse", Lanzarote, 25 October 2007. Available at *http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=201&CM=8&DF=&CL=ENG*

Council of Europe (2008a), Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters (Adopted by the Committee of Ministers on 26 March 2008 at the 1022nd meeting of the Ministers' Deputies), Available at *https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2008)6&Language=lanEnglish&Site=CM&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864*

Council of Europe (2008b), *The Internet Literacy Handbook. A guide for parents, teachers and young people*, 3rd edition. Available at *www.coe.int/t/dghl/standardsetting/internetliteracy/hbk_EN.asp*

Council of Europe (2008c), Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children on the Internet (Adopted by the Committee of Ministers on 20 February 2008 at the 1018th meeting of the Ministers' Deputies). Available at *https://wcd.coe.int/ViewDoc.jsp?id=1252427&Site=CM*

Council of Europe (2009), Recommendation CM/Rec(2009)5 of the Committee of Ministers to member states on measures to protect children against harmful content and behaviour and to promote their active participation in the new information and communications environment (Adopted by the Committee of Ministers on 8 July 2009 at the 1063rd meeting of the Ministers' Deputies). Available at *https://wcd.coe.int/ViewDoc.jsp?id=1470045&Site=CM*

De Haan, J. and Livingstone, S. (2009), "Policy and research recommendations". LSE, London: EU Kids Online (Deliverable D5). Available at *www.lse.ac.uk/collections/EUKidsOnline/Reports/D5Recommendations.pdf*

Deloitte Enterprise Risk Services (2008), "Test and benchmark of products and services to voluntarily filter Internet content for children between 6 and 16 years". Synthesis Report 2008 Edition. Report prepared for the European Commission. Available at *www.sip-bench.org/Reports2008/sip_bench_2008_synthesis_report_en.pdf*

Donoso, Veronica, Leen D'haenens, Bieke Zaman, Anna Van Cauwenberge and Katia Segers (2008), National Report for Belgium, in: Cross-national Comparisons for EU Kids *Online,* Available at *www.lse.ac.uk/collections/EUKidsOnline/Reports/WP3NationalReportBelgium.pdf*

Dooley, J.J., Cross, D., Hearn, L. and Treyvaud, R. (2009), "Review of existing Australian and international cyber-safety research". Child Health Promotion Research Centre, Edith Cowan University, Perth. Available at *www.dbcde.gov.au/__data/assets/pdf_file/0004/119416/ECU_Review_of_existing_Australian_and_international_cyber-safety_research.pdf*

eNacso (2009), "Developing a Response to a new breed of location services". Available at *www.enacso.eu/index.php?option=com_rokdownloads&view=file&task=download&id=8%3Aenacso-response-to-the-new-breed-of-location-services&Itemid=11*

Enex TestLab (2009), "Internet Service Provider Content Filtering Pilot Report". Available at *www.dbcde.gov.au/__data/assets/pdf_file/0008/123857/Enex_Testlab_report_into_ISP-level_filtering_-_01_Main_report.pdf*

ENISA (2007), "Security Issues and Recommendations for Online Social Networks". ENISA Position Paper No.1. Available at *www.enisa.europa.eu/act/res/other-areas/social-networks/security-issues-and-recommendations-for-online-social-networks/at_download/fullReport*

ENISA (2008), "Security and Privacy in Massively-Multiplayer Online Games and Social and Corporate Virtual Worlds. Virtual Worlds, Real Money". Position Paper. Available at *www.enisa.europa.eu/act/it/oar/massively-multiplayer-online-games-and-social-and-corporate-virtual-worlds/security-and-privacy-in-virtual-worlds-and-gaming*

European Association of Communications Agencies (2006), "Ethical Guidelines for Advertising to Children". Available at *www.eaca.be/_upload/documents/guidelines/Ethical%20guidelines%20for%20Advertising%20and%20Children.doc*

EC (European Commission) (2006), "Flash Eurobarometer (EU25). Safer Internet". Available at *http://ec.europa.eu/information_society/activities/sip/docs/eurobarometer/eurobarometer_2005_25_ms.pdf*

EC (2008a), Public Consultation Age Verification, Cross Media Rating and Classification, Online Social Networking; Belgian Awareness Node; Questionnaire 1; Available at *http://ec.europa.eu/information_society/activities/sip/docs/pub_consult_age_rating_sns/results/crioc_a531786.pdf*

EC (2008b), "Background Report on Cross Media Rating and Classification and Age Verification Solutions". Safer Internet Forum 2008. Available at *http://ec.europa.eu/information_society/activities/sip/docs/pub_consult_age_rating_sns/reportageverification.pdf*

EC (2008c), "Flash Eurobarometer (EU27). Towards a safer use of the Internet for children in the EU – a parents' perspective", analytical report. Available at *http://ec.europa.eu/information_society/activities/sip/docs/eurobarometer/analyticalreport_2008.pdf*

EC (2009a), "Empowering and Protecting Children online". Available at *http://ec.europa.eu/information_society/doc/factsheets/018-safer-internet.pdf*

EC (2009b), Communications COM (2009) 64 final. Final evaluation of the implementation of the multiannual Community Programme on promoting safer use of the Internet and new online technologies. Brussels, 18.2.2009. Available at *http://ec.europa.eu/information_society/activities/sip/docs/prog_evaluation/comm_final_eval_sip_en_2005_2008.pdf*

European Framework for Safer Mobile Use by Younger Teenagers and Children, February 2007. Available at *http://ec.europa.eu/information_society/activities/sip/docs/mobile_2005/europeanframework.pdf*

European Parliament and Council (2006), Recommendation 2006/952/EC of the European Parliament and of the Council of 20 December 2006 on the protection of minors and human dignity and on the right of reply in relation to the competitiveness of the European audiovisual and on-line information services industry. Available at *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006H0952:EN:NOT*

European Parliament and Council (2007), Directive 2007/65/EC of the European Parliament and of the Council of 11 December 2007 amending Council Directive 89/552/EEC on the co-ordination of

certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities (Audiovisual Media Services Directive). Available at *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32007L0065:EN:NOT*

EURYDICE (2009), "Education on Online Safety in Schools in Europe". Summary Report. Available at *http://eacea.ec.europa.eu/education/eurydice/documents/thematic_reports/121EN.pdf*

FOSI (Family Online Safety Institute) (2007), "State of Online Safety Report 2008". Available at *http://fosi.org/cms/downloads/policy/online_safety_report08.pdf*

Fielder, A., Gardner, W., Nairn and A., Pitt, J. (2007), "Fair game? Assessing commercial activity on children's favourite Web sites and online environments". Available at *www.agnesnairn.co.uk/policy_reports/fair_game_final.pdf*

Government of Canada (2000), "Illegal and Offensive Content on the Internet. Canadian Strategy to Promote Safe, Wise and Responsible Internet Use". Available at *http://dsp-psd.pwgsc.gc.ca/Collection/C2-532-2000E.pdf*

Grimm, P., Rhein, St. and Clausen-Muradian, E. (2008), Gewalt im Web 2.0. Der Umgang Jugendlicher mit gewalthaltigen Inhalten und Cyber- Mobbing sowie die rechtliche Einordnung der Problematik, Schriftenreihe der NLM; Bd. 23, Berlin: Vistas Verlag. Available at *www.nlm.de/fileadmin/dateien/aktuell/Studie_Prof._Grimm.pdf*

Hans-Bredow-Institut and the Institute of European Media Law (2006), Final Report. Study on Co-Regulation Measures in the Media Sector. Study for the European Commission. Available at *http://ec.europa.eu/avpolicy/docs/library/studies/coregul/final_rep_en.pdf*

Hasebrink, U., Livingstone, S., Haddon, L. and Ólafsson, K. (2009), "Comparing children's online opportunities and risks across Europe: Cross-national comparisons for EU Kids Online". LSE, London: EU Kids Online (Deliverable D3.2, 2nd edition).

IIA (Internet Industry Association) (2008), Feasibility Study - ISP Level Content Filtering, February 2008; Main report, Available at *www.dbcde.gov.au/__data/assets/pdf_file/0006/95307/Main_Report_-_Final.pdf*

ISTTF (Internet Safety Technical Task Force) (2008), "Enhancing Child Safety and Online Technologies": Final Report of the ISTTF to the Multi-State Working Group on Social Networking of State Attorney Generals of the United States. Cambridge, MA: Berkman Center for Internet and Society, Harvard University. Available at *http://cyber.law.harvard.edu/pubrelease/isttf/*

ITU (2009a), "Guidelines for Policy Makers of Child Online Protection". Available at *www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/policy_makers.pdf*

ITU (2009b), Tokyo Communiqué on Safer Internet Environment for Children as agreed by participants to the ITU/ MIC Strategic Dialogue on "Safer Internet Environment for Children" on 3 June 2009 in Tokyo, Japan. Available at *www.itu.int/osg/csd/cybersecurity/gca/cop/meetings/june-tokyo/documents/ITU-Tokyo-Communique.doc.*

ITU (2010a), Council Working Group on Child Online Protection. The Source of Online Threats to Youth and Children. Geneva, 11 June 2010. Available at *www.itu.int/council/groups/wg-cop/second-meeting-june-2010/010610_Online_Threats_COP_Rev.1.doc*

ITU (2010b), Child Online Protection. Statistical Framework and Indicators. Available at *www.itu.int/pub/D-IND-COP.01-11-2010/en*

Jakubowicz, Karol (2009), "A New Notion of Media. Media and media-like content and activities on new communication services". Background Text. First Council of Europe Conference of Ministers Responsible for the Media and New Communications Services.

Kaiser Family Foundation (2006), It's Child's Play: Advergaming and the Online Marketing of Food to Children. Available at *www.kff.org/entmedia/upload/7536.pdf*

Kaiser Family Foundation (2010), Generation M2, Media in the Lives of 8-Year-Olds. Available at *www.kff.org/entmedia/upload/8010.pdf*

KJM (Komission für Jugendmedienshutz der Landesmedienanstalten) (2009), Interstate Treaty on the Protection of Minors in Broadcasting and Telemedia. Available at *www.alm.de/fileadmin/Download/Gesetze/JMStV_Stand_11.RStV_englisch.pdf*

Lee, Byeong Gi (Commissioner, Korea Communications Commission, 2009), Understanding Korea's "Identity Verification System". Available at *http://121.254.145.213/gisa_down.php?pfile=%2Fdata1%2Fftp%2Fgisa_download%2F20091206_%C2%FC%B0%ED%C0%DA%B7%E1_Identity+Verification+System+2009.12.+BGL.doc*

Livingstone, S. and Bober, M. (2005), "UK children go online: Final report of key project findings". London: LSE Research Online. Available at *http://eprints.lse.ac.uk/399/*

Livingstone, S., and Haddon, L. (2009), "EU Kids Online: Final report". LSE, London: EU Kids Online. (EC Safer Internet Plus Programme Deliverable D6.5). Available at *www.lse.ac.uk/collections/EUKidsOnline/Reports/EUKidsOnlineFinalReport.pdf*

Livingstone, S. (2009), "A Rationale for Positive Online Content for Children". *Communication Research Trends*, Volume 28, No. 3, p. 12.

Marwick, A., Murgia-Diaz, D. and Palfrey, J. (2010), "Youth, Privacy and Reputation" (Literature Review), *Berkman Center Research* Publication No. 2010-5. Available at *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1588163*

Media Awareness Network (2005), "Young Canadians in a Wired World: Phase II Trends and Recommendations". Available at *www.media-awareness.ca/english/research/YCWW/phaseII/upload/YCWWII_trends_recomm.pdf*

Millwood Hargrave, A. (2009), "Protecting children from harmful content". Report prepared for the Council of Europe's Group of Specialists on Human Rights in the Information Society. Available at www.coe.int/t/dghl/standardsetting/media/Doc/H-Inf(2009)13_en.pdf

Millwood Hargrave, A., Livingstone, S., *et al.,* (2009). *Harm and Offense in Media Content: A Review of the Empirical Literature*. 2nd ed., Bristol Intellect Press.

Muir, D. (2005), *Violence Against Children in Cyberspace: A Contribution to the United Nations Study on Violence Against Children*. Bangkok, Thailand: ECPAT International. Available at www.ecpat.net/EI/Publications/ICT/Cyberspace_ENG.pdf#

National Consumer Council (2007), "Watching, wanting and wekkbeing: exploring the links". Available at: *www.agnesnairn.co.uk/policy_reports/watching_wanting_and_wellbeing_july_2007.pdf*

New Zealand's Department of Internal Affairs (n.d.), "Censorship and the Internet". Available at *www.dia.govt.nz/diawebsite.nsf/Files/Censorship_Internet/$file/Censorship_Internet.pdf*

NICC (2008), "Notice and Take Down Code of Conduct". Available at *www.samentegencybercrime.nl/UserFiles/File/NTD_Gedragscode_Opmaak_Engels.pdf*

Nordic Consumer Affairs Ministers (n.d.), "Internet Marketing Aimed at Children and Minors". Resolution by the Nordic consumer affairs ministers. Available at *www.kuluttajavirasto.fi/File/71c7279a-af1a-4cea-b858-ae7948ca96d8/Internet+marketing+aimed+at+children+and+minors.pdf*

O'Connell, R., and Bryce, J. (2006), "Young People, Well-Being and Risk On-Line". Strasbourg: Media Division, Directorate General of Human Rights, Council of Europe. Available at *www.coe.int/t/dghl/standardsetting/media/Doc/H-Inf(2006)005_en.pdf*

OECD (1980), "Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data". Available at: *www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html*

OECD (1999), "Approaches to Content on the Internet". DSTI/ICCP(97)14/FINAL, OECD, Paris. Available at: *www.oecd.org/officialdocuments/displaydocumentpdf?cote=DSTI/ICCP(97)14/FINAL*

OECD (2001), *The DAC Guidelines, Poverty Reduction*, OECD, Paris. Available at *www.oecd.org/dataoecd/47/14/2672735.pdf.*

OECD (2002), *Regulatory Policies in OECD Countries. From Interventionism to Regulatory Governance*. OECD, Paris.

OECD (2003), "Policy Coherence: Vital for Global Development". Policy Brief, OECD, Paris. Available at *www.oecd.org/dataoecd/1/50/8879954.pdf*

OECD (2006), "Mobile Commerce". OECD Digital Economy Paper 124, Directorate for Science, Technology and Industry, OECD, Paris. Available at *www.oecd.org/dataoecd/22/52/38077227.pdf*

OECD (2007a), *Participative Web and User-Created Content: Web 2.0, Wikis and Social Networking*. OECD, Paris.

OECD (2007b), Working Party on Regulatory Management and Reform: Methodological Guidance and Frameworks for RIA, GOV/PGC/REG(2007)8.

OECD (2008), "The Seoul Declaration for the Future of the Internet Economy". Available at *www.oecd.org/dataoecd/49/28/40839436.pdf*

OECD (2009a), "Report on the APEC-OECD Joint Symposium on Initiatives among Member Economies Promoting Safer Internet Environment for Children". Available at *www.oecd.org/dataoecd/46/46/44120262.pdf*

OECD (2009b), *Computer Viruses and Other Malicious Software. A Threat to the Internet Economy*. OECD, Paris. Available at *www.oecd.org/document/16/0,3343,en_2649_34223_42276816_1_1_1_37441,00.html*

OECD (2009c), "The Economic and Social Role of Internet Intermediaries". OECD Digital Economy Papers 171, Directorate for Science, Technology and Industry, OECD, Paris. Available at *www.oecd.org/dataoecd/49/4/44949023.pdf*

OECD (2010a). "National Strategies and Policies for Digital Identity Management in OECD Countries". OECD Digital Economy Paper 177, Directorate for Science, Technology and Industry, OECD, Paris

OECD (2010b), The role of Internet Intermediaries in Advancing Public Policy Objectives. Forging Partnership for Advancing Policy Objectives for the Internet Economy, Part II and III. ICCP(2010)11, OECD, Paris.

OECD (2010c), "Conference on Empowering E-consumers: Strengthening Consumer Protection in the Internet Economy- Summary of key points and conclusions". DSTI/CP(2010)2/FINAL, OECD, Paris.

OECD (2010d), "The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines". DSTI/ICCP/REG(2010)6/FINAL. OECD, Paris.

OECD (2010e), "Ministerial report on the OECD Innovation Strategy. Innovation to strengthen growth and address global and social challenges". May 2010, OECD, Paris. Available at *www.oecd.org/dataoecd/51/28/45326349.pdf*

OECD (2010f), "The role of Internet Intermediaries in Advancing Public Policy Objectives". Workshop Summary, 16 June 2010, Paris, France. Available at *www.oecd.org/dataoecd/8/59/45997042.pdf*

Ofcom (2007), "Ofcom's Submission to the Byron Review, Annex 5: The Evidence Base – The views of Children, Young People and Parents". Available at: *www.ofcom.org.uk/research/telecoms/reports/byron/annex5.pdf*

Ofcom (2008a), "Social Networking: A quantitative and qualitative research report into attitudes, behaviours and use". Available at *http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/report1.pdf*

Ofcom (2008b), "UK code of practice for the self-regulation of new forms of content on mobiles", Review 2008, Available at *www.ofcom.org.uk/advice/media_literacy/medlitpub/ukcode/ukcode.pdf*

Ofcom (2008c), "Ofcom's Response to the Byron Review, Statement 2008", Available at *http://stakeholders.ofcom.org.uk/binaries/research/telecoms-research/Byron_exec_summary.pdf*

Ofcom (2010), "UK children's media literacy". Available at *http://stakeholders.ofcom.org.uk/binaries/research/media-literacy/ukchildrensml1.pdf*

Online Safety and Technology Working Group (OSTWG) (2010), "Youth Safety in a Living Internet: Report of the Online Safety and Technology Working Group", 4 June 2010, p. 16. Available at *www.ntia.doc.gov/reports/2010/OSTWG_Final_Report_060410.pdf*

PEGI Online (n.d.), PEGI Online Safety Code (POSC), "A Code of Conduct for the European Interactive Software Industry". Available at *www.pegionline.eu/en/index/id/235/media/pdf/197.pdf*

Peter, J., Valkenburg, P. M., and Schouten, A. P. (2006), "Characteristics and Motives of Adolescents Talking with Strangers on the Internet". *CyberPsychology & Behavior*, 9(5), 526-530.

Pew Internet & American Life Project (2007), "Teens, Privacy & Online Social Networks. How teens manage their online identities and personal information in the age of MySpace". Available at *www.pewinternet.org/~/media//Files/Reports/2007/PIP_Teens_Privacy_SNS_Report_Final.pdf*

Pew Internet & American Life Project (2009), "Teens and Sexting. How and why minor teens are sending sexually suggestive nude or nearly nude images via text messaging". Available at *http://pewInternet.org/Reports/2009/Teens-and-Sexting.aspx.*

Pew Internet & American Life Project (2010), "Reputation Management and Social Media. How people monitor and maintain their identity through search and social media". Available at *http://pewinternet.org/Reports/2010/Reputation-Management/Summary-of-Findings.aspx?r=1.*

Powell, Alison, Hills, Michael, and Nash, Victoria (2010), "Child Protection and Freedom of Expression Online". *Oxford Internet Institute Forum Discussion Paper No. 17*, 1 March 2010. Available at *www.oii.ox.ac.uk/publications/FD17.pdf*

PricewaterhouseCoopers (2009), "European Framework for Safer Mobile Use by Younger Teenagers and Children". Available at *www.gsmeurope.org/documents/PwC_Implementation_Report.pdf*

Safer Internet Programme (2010), "Assessment Report on the Status on Online Safety Education in Schools across Europe". Available at *http://ec.europa.eu/information_society/activities/sip/docs/forum_oct_2009/assessment_report.pdf*

Safer Social Networking Principles for the EU (2009), Available at *http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf*

Schmidt, Marie E. and Vandewater , Elizabeth A. (2008), "Media and Attention, Cognition, and School Achievement", *Children and Electronic Media*, Vol. 18, No 1, Spring 2008. Available at *http://ccf.tc.columbia.edu/pdf/Children%20and%20Electronic%20Media_Spring%2008.pdf*

Shafer, Joseph A. (2002), "Spinning the Web of Hate: Web-based Hate Propagation by Extremist Organizations", *Journal of Criminal Justice and Popular Culture*, 9 (2): 69-88. Available at *www.albany.edu/scj/jcjpc/vol9is2/schafer.pdf*

Solove, Daniel J. (2007), "The Future of Reputation: Gossip, Rumor, and Privacy on the Internet". *Yale University Press*. Available at *http://docs.law.gwu.edu/facweb/dsolove/Future-of-Reputation/text.htm*

Staksrud, Elisabeth and Lobe, Bojana (2010), "Evaluation of the Implementation of the Safer Social Networking Principles for the EU Part I: General Report". Available at *http://ec.europa.eu/information_society/activities/social_networking/docs/final_report/first_part.pdf*

Stross, R. (2010), "Computers at Home: Educational Hope vs. Teenage Reality". *The New York Times*. Published on 9 July 2010. Available at: *www.nytimes.com/2010/07/11/business/11digi.html.*

Thierer, A. (2009a), "Parental Controls & Online Child Protection: A Survey of Tools & Methods". Washington, D. C.: The Progress & Freedom Foundation. Available at *www.pff.org/parentalcontrols/*

Thierer, A. (2009b), "Five Online Safety Task Forces Agree: Education, Empowerment & Self-Regulation are the Answer". Progress & Freedom Foundation Progress on Point Paper, Vol. 16, No. 13, July 2009. Available at *http://ssrn.com/abstract=1433504*

TACD (Trans Atlantic Consumer Dialogue) (2009), "Resolution on Marketing to Children Online", Available at *http://tacd.org/index2.php?option=com_docman&task=doc_view&gid=207&Itemid*

UKCCIS (UK Council for Child Internet Safety) (2009), "Click Clever, Click Safe: The First Child Internet Safety Strategy. Available at *www.dcsf.gov.uk/ukccis/news_detail.cfm?newsid=36&thisnews=2*

UK Department for Children, Schools and Families, and Department for Culture, Media and Sport (2009), "The Impact of the Commercial World on Children's Wellbeing: Report of an Independent Assessment". Available at *http://publications.dcsf.gov.uk/eOrderingDownload/00669-2009DOM-EN.pdf*

UK Home Office (2005), "Good Practice Guidance for the Moderation of Interactive Services for Children", Available at *http://police.homeoffice.gov.uk/publications/operational-policing/moderation-document-final.pdf*

UK Home Office (2008), "Good Practice Guidance for the providers of social networking and other user interactive services 2008". Available at *http://police.homeoffice.gov.uk/publications/operational%2Dpolicing/social%2Dnetworking%2Dguidance*

United Nations (1989), "Convention on the Rights of the Child Adopted and opened for signature", ratification and accession by General Assembly resolution 44/25 of 20 November 1989. Available at *www2.ohchr.org/english/law/pdf/crc.pdf*

US Department of Justice (2002), *Drug, Youth and the Internet*. Available at *www.justice.gov/ndic/pubs2/2161/2161p.pdf*

US FCC (Federal Communications Commission) (2009), "In the Matter of Implementation of the Child Safe Viewing Act; Examination of Parental Control Technologies for Video or Audio Programming", MB Docket No. 09-26. Available at *http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-09-69A1.pdf.*

US FTC (Federal Trade Commission) (n.d.), "Children's Online Privacy Protection Rule"; Final Rule, 16 CFR Part 312.

US FTC (2002), "Protecting Children's Privacy Under COPPA: A Survey on Compliance". Staff Report, Available at *www.ftc.gov/os/2002/04/coppasurvey.pdf.*

US FTC (2007), "Implementing the Children's Online Privacy Protection Act". A Report toCongress, February 2007. Available at *www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf*

US FTC (2009a), "Beyond Voice: Mapping the Mobile Marketplace". Staff Report. Available at *www.ftc.gov/reports/mobilemarketplace/mobilemktgfinal.pdf*

US FTC (2009b), "Virtual Worlds and Kids: Mapping the Risk". A Report to Congress, December 2009. Available at *www.ftc.gov/os/2009/12/oecd-vwrpt.pdf*

US FTC (2010), "FTC Seeks Comment on Children's Online Privacy Protections; Questions Whether Changes to Technology Warrant Changes to Agency Rule". Available at *www.ftc.gov/opa/2010/03/coppa.shtm*

Valkenburg, Patti M., and Peter, Jochen (2008), "Adolescents' Identity Experiments on the Internet: Consequences for Social Competence and Self-Concept Unity", Communication Research, (2008) 35, p. 208.

Wolak, J., Finkelhor, D., and Mitchell, K. (2006), "Online Victimization of Youth: Five years Later". Available at *www.unh.edu/ccrc/pdf/CV138.pdf*

Wolak, J., Finkelhor, D., and Mitchell, K. (2007), "1 in 7 youth: The statistics about online solicitations". Available at *http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/1in7Youth.pdf*

Woollard, J., Wickens, C., Powell, K. and Russell, T. (2007), "E-safety: evaluation of key stage 3 materials for initial teacher education: Childnet International".

Yahoo! and Carat Interactive (2003), "Born to be wired, the Role of New Media for a Digital Generation". Available at *http://us.i1.yimg.com/us.yimg.com/i/promo/btbw_2003/btbw_execsum.pdf*

YPRT (Youth Protection Roundtable) (2009), *Stiftung Digitale Chancen*. Youth Protection Toolkit. Available at *www.yprt.eu/transfer/assets/final_YPRT_Toolkit.pdf*