Keeping children safe online has been the subject of intensive policy debate ever since the mid-1990s when the internet first became an important public communications medium. The European Union has been to the fore in promoting internet safety and through its Safer Internet Programme has supported multi-stakeholder initiatives with industry, law enforcement, education and civil society to create a safer internet environment. Now, with a new emphasis on not just a safer but also a better internet, policy makers have signalled a new phase in strategies to protect children online. Reviewing the development of internet safety policy over this period – against the background of better evidence about the reality of young people’s experiences – and looking to its future are among the key themes of this book.

Contributors, all members of the now 33-country EU Kids Online network, seek to add to a growing literature on policy matters regarding internet regulation and governance as the Internet enters a new phase of maturity with near universal access and use. European in scope but international in outlook, the chapters in this collection seek to raise critical debate on just how mainstream are policies to protect young people, promote their best interests online and empower them to avail of the full range of digital opportunities? Against a background of increased international tension and debate over whether the internet should be regulated at all, contributors adopt a somewhat different position and assess the forms, contexts and evidence in favour of action – regulatory and otherwise – needed to support safer and better outcomes for young people.
NORDICOM’s activities are based on broad and extensive network of contacts and collaboration with members of the research community, media companies, politicians, regulators, teachers, librarians, and so forth, around the world. The activities at Nordicom are characterized by three main working areas.

- **Media and Communication Research Findings in the Nordic Countries**
  Nordicom publishes a Nordic journal, *Nordicom Information*, and an English language journal, *Nordicom Review* (refereed), as well as anthologies and other reports in both Nordic and English languages. Different research databases concerning, among other things, scientific literature and ongoing research are updated continuously and are available on the Internet. Nordicom has the character of a hub of Nordic cooperation in media research. Making Nordic research in the field of mass communication and media studies known to colleagues and others outside the region, and weaving and supporting networks of collaboration between the Nordic research communities and colleagues abroad are two prime facets of the Nordicom work.

  The documentation services are based on work performed in national documentation centres attached to the universities in Aarhus, Denmark; Tampere, Finland; Reykjavik, Iceland; Bergen, Norway; and Göteborg, Sweden.

- **Trends and Developments in the Media Sectors in the Nordic Countries**
  Nordicom compiles and collates media statistics for the whole of the Nordic region. The statistics, together with qualified analyses, are published in the series, *Nordic Media Trends*, and on the homepage. Besides statistics on output and consumption, the statistics provide data on media ownership and the structure of the industries as well as national regulatory legislation. Today, the Nordic region constitutes a common market in the media sector, and there is a widespread need for impartial, comparable basic data. These services are based on a Nordic network of contributing institutions.

  Nordicom gives the Nordic countries a common voice in European and international networks and institutions that inform media and cultural policy. At the same time, Nordicom keeps Nordic users abreast of developments in the sector outside the region, particularly developments in the European Union and the Council of Europe.

- **Research on Children, Youth and the Media Worldwide**
  At the request of UNESCO, Nordicom started the International Clearinghouse on Children, Youth and Media in 1997. The work of the Clearinghouse aims at increasing our knowledge of children, youth and media and, thereby, at providing the basis for relevant decision-making, at contributing to constructive public debate and at promoting children’s and young people’s media literacy. It is also hoped that the work of the Clearinghouse will stimulate additional research on children, youth and media. The Clearinghouse’s activities have as their basis a global network of 1000 or so participants in more than 125 countries, representing not only the academia, but also, e.g., the media industries, politics and a broad spectrum of voluntary organizations.

  In yearbooks, newsletters and survey articles the Clearinghouse has an ambition to broaden and contextualize knowledge about children, young people and media literacy. The Clearinghouse seeks to bring together and make available insights concerning children’s and young people’s relations with mass media from a variety of perspectives.

[www.nordicom.gu.se](http://www.nordicom.gu.se)
Towards a Better Internet for Children?
## Contents

Acknowledgements

*Neelie Kroes, Vice-President of the European Commission*

Foreword

*Brian O’Neill, Elisabeth Staksrud & Sharon McLaughlin*

Introduction

PART I POLICY PILLARS

Chapter 1
*Elisabeth Staksrud & Jørgen Kirksæther*
Filtering & Content Classification

Chapter 2
*Brian O’Neill*
Internet Hotlines. A Reporting Solution for Internet Safety?

Chapter 3
*Elisabeth Staksrud & Kjartan Ólafsson*
Awareness. Strategies, Mobilisation and Effectiveness

Chapter 4
*Sharon McLaughlin*
Regulation and Legislation

Chapter 5
*Sonia Livingstone*
‘Knowledge Enhancement’. The Risks and Opportunities of Evidence-based Policy

Chapter 6
*Jos de Haan, Simone van der Hof, Wim Bekkers & Remco Pijpers*
Self-Regulation

PART II POLICY PLAYERS

Chapter 7
*Brian O’Neill*
The Changing Role of the Media Regulator

7

9

11

23

39

57

77

93

111

133
Chapter 8
*Bence Ságvári & Miklós Péter Máder*
Industry. Towards the Socially Responsible Internet.
Industry CSR Practices Across Europe 153

Chapter 9
*Tatjana Taraszow*
The Influence of NGOs on Safer Internet Policy Making 173

Chapter 10
*Brian O’Neill & Yiannis Laouris*
Teaching Internet Safety, Promoting Digital Literacy.
The Dual Role of Education and Schools 193

Chapter 11
*Giovanna Mascheroni, Maria Francesca Murru, Elena Aristodemou & Yiannis Laouris*
Parents. Mediation, Self-regulation and Co-regulation 211

Chapter 12
*Monica Barbouschi & Valentina Marinescu*
Youth. Revisiting Policy Dilemmas in Internet Safety in the
Context of Children’s Rights 227

PART III POLICY PARADOXES

Chapter 13
*Leen d’Haenens & Liza Tsaliki*
Risk versus Harm. Children’s Coping Profiles 249

Chapter 14
*Andrea Duerager, Sonja Duerager & Ingrid Paus-Hasebrink*
Protection versus Privacy. An Area of Conflict 267

Chapter 15
*Uwe Hasebrink & Bojana Lobe*
The Cultural Context of Risk. On the Role of Intercultural
Differences for Safer Internet Issues 283

Chapter 16
*Sharon McLaughlin*
Rights v. Restrictions. Recognising Children’s Participation in
the Digital Age 301

Index 321

The Contributors 329
Acknowledgements

The editors would like to acknowledge the valuable support of the Dublin Institute of Technology and the Department of Media and Communication, University of Oslo. We would also like to thank all our research colleagues in the EU Kids Online network, as well as our colleagues in the wider Safer Internet field in Europe and beyond. Finally we would like to thank all the children and parents who willingly have answered all our survey questions, providing the basis for all our work.
As the European Commissioner for the Digital Agenda, my aim is to ensure that all Europeans, children and adults have the access, skills, competences and trust to enjoy better online content and services.

I want children to be safe and protected when they are online. But I want to go beyond that. Every child and every student needs to be equipped with the necessary skills to climb further up the ladder of digital opportunities.

By encouraging creativity online, we can help kids make positive use of the internet. If we help children and young people to develop their digital skills, they can make the most of the online world, with the abilities and tools to learn, participate, and have fun online. As the EU Kids Online survey points out, schools are best equipped to teach these important skills. Universities and the technology industry have to contribute as well and work together to achieve this.

The EU Kids Online network has provided a valuable insight into children’s use of online technologies. We know better now about how children use the Internet, the risks they encounter online and their online safety. The EU Kids Online network has provided the underpinning evidence base for every actor working in the area of online safety. EU Kids Online findings helped us to shape the *European Strategy for a Better Internet for Children*.

The world is changing in so many ways. Disruptive technologies, as well as societal and economic changes pose many challenges. In order to face them actions are needed at a European level. Stakeholders need to join up not only their forces, but also to work towards the right approaches and partnerships towards a better internet for children. But we also need to involve children and young people to tell us and show us how we can create a better internet with them.
Europeans will not embrace technology they do not trust – the digital age is neither “big brother” nor “cyber wild west”.

_A Digital Agenda for Europe_ (European Commission 2010)

Keeping children safe online has been the subject of intensive policy debate ever since the mid-1990s when the internet first became an important public communications medium. The European Union has been to the fore in promoting internet safety and through its Safer Internet Programme has supported multi-stakeholder initiatives with industry, law enforcement, education and civil society to create a safer internet environment. Now, with a new emphasis on not just a safer but also a better internet (European Commission 2012), policy makers have signalled a new phase in strategies to protect children online. Reviewing the development of internet safety policy over this period – against the background of better evidence about the reality of young people’s experiences – and looking to its future are among the key themes of this book.

Since 2006, EU Kids Online, a research network supported by the European Union’s Safer Internet Programme, has monitored children’s and parents’ experiences of the internet across Europe, examining their access to internet technologies, the uses and activities undertaken, the risks young people encounter and the impact this has on them. The first EU Kids Online project, from 2006-2009, resulted in a series of reports, a research database, as well as the book, _Kids Online: Opportunities and Risks for Children_ (Livingstone and Haddon 2009) that assessed the available evidence and classified online opportunities and risks facing children. EU Kids Online II (2009-11) through its unique pan-European survey produced new evidence regarding risk and safety online for children and parents in 25 countries across Europe. It developed a theoretically-informed, comparative analysis of children’s online experiences and coping strategies when dealing with problematic situations. Through detailed analysis of factors underpinning risk and harm, the project sought to inform policy decisions and
assist in more effective policy formation on internet safety. Research arising from this project resulted in a series of detailed reports as well as the publication of the book *Children, risk and safety online: Research and policy challenges in comparative perspective* (Livingstone, Haddon *et al.* 2012).

Strengthening knowledge about this fast-moving environment in order to inform policy on safer internet practices has been a core objective throughout. The network has tested taken-for-granted assumptions regarding the nature, extent and interpretation of online risk, the nature and degree of children’s internet literacy and the effectiveness of parental regulation. It has actively contributed to policy making through stakeholder engagement, publishing several reports on policy recommendations and implications (O’Neill and McLaughlin 2010; O’Neill, Livingstone, *et al.* 2011) and ensuring that research findings have been widely disseminated in both national and European contexts.

The current volume continues this work in policy discussion and debate. Contributors, all members of the now 33-country EU Kids Online network, seek to add to a growing literature on policy matters regarding internet regulation and governance as the Internet enters a new phase of maturity with near universal access and use. European in scope but international in outlook, the chapters in this collection seek to raise critical debate on just how mainstream are policies to protect young people, promote their best interests online and empower them to avail of the full range of digital opportunities? Against a background of increased international tension and debate over whether the internet should be regulated at all, contributors adopt a somewhat different position and assess the forms, contexts and evidence in favour of action – regulatory and otherwise – needed to support safer and better outcomes for young people.

**Revisiting Policy**

Within the EU/EEA (European Economic Area), policy in relation to the overriding issues of public interest – the protection of minors, protection of human dignity, information security, protection of privacy, and so on – date back to 1996 when the European Parliament and Council called on the Commission to examine in-depth the issues related to the development of new audiovisual and information services. The Commission responded with two key texts: the *Green Paper On The Protection Of Minors And Human Dignity in Audiovisual and Information Services* (European Commission 1996), setting out debate on a medium to long term basis on how to achieve protection of young people in this new communications environment, while the accompanying Communication on *Illegal and Harmful Content on the Internet* (European Commission 1996) took up immediate practical measures to tackle the use of the internet for illegal activities.
The potential of the internet to transform Europe’s economy and to create unparalleled social, cultural and educational benefits for its citizens as articulated in the Bangemann report of 1994, *Europe and the Global Information Society*, provides a fundamental political motivation for Europe’s Information Society policies. As the social agenda of digital inclusion has increased in prominence, however, so too has the question of internet safety. Persistent problems of the distribution of child abuse material online, the potential threat of paedophile grooming, the unregulated access to numerous kinds of content that may be harmful for young people’s development, cyberbullying, unwanted contact and inadequate skills among users have cast a shadow over the many opportunities the internet offers Europe’s young citizens. The unprecedented growth of the internet and the rapid diffusion of ever more sophisticated networking technologies frequently outpace the ability of governments and policy makers everywhere to anticipate its consequences. Regulation in the traditional sense of controlling by legislation and placing restrictions on market forces has been perceived as antithetical to the flourishing digital economy which all governments seek to support. As a consequence, a variety of voluntary and cooperative forms of regulation between industry stakeholders and government interests have sought to create the optimal conditions for innovation and development of digital opportunities while sensitive to any potentially negative social consequences.

An inclusive society in which equal digital opportunities exist for all requires at its foundation trust and confidence in the safety of the online world and protection of the most vulnerable members and citizens. Europeans, as suggested in *A Digital Agenda for Europe*, will not embrace technology they do not trust, especially if they view it as a “big brother” threat or a “cyber wild west” (European Commission 2010). Consequently, successive phases of the European Commission’s Safer Internet Programme have, since 1999, sought to foster greater trust through awareness raising and education initiatives aimed at parents, educators and children; industry involvement in safety enhancement; supporting the production of online content dedicated to the needs of children; and promoting initiatives to tackle the spread of illegal content.

Online safety was one of the headline themes of the inaugural Digital Agenda Assembly of 2011 under the slogan ‘Every European child safe online’. Achievements over the previous decade were impressive: self-regulatory codes of practice in the areas of mobile communications and in social networking had the support of all the major technology companies in Europe with successive evaluations showing signs of success. The INHOPE network of European hotlines, set up for the reporting of illegal content online, had expanded to 43 member organisations in 37 countries (Insafe-INHOPE 2013). The PEGI age rating system for video games had rapidly gained wide industry support and was increasingly used for online gaming also as a trusted source of information for
parents and users on age-appropriateness of video game content.5 The annual Safer Internet Day, inaugurated in 2004 as an initiative of the EU SafeBorders project and now organised by Insafe, the network of internet safety awareness centres in Europe, has helped to raise the profile of safe and responsible use of internet and mobile technologies on a global scale.6 With Safer Internet Centres, originally initiated by the SAFT project in 2002 and now present in all 27 member states plus Iceland, Norway and Russia, typically comprising a combined awareness centre, helpline, hotline and youth panel, there is now a consolidated infrastructure across Europe reinforcing at national level, pan-European approaches to safer internet practices and policies. Likewise, the Safer Internet Forum, organised as an annual conference since 2004 hosted by the European Commission, has been an opportunity to showcase progress on safer internet issues and over the years has highlighted developments in industry codes of conduct, risks and mobile technologies, age verification and social networking, promoting online safety in schools, and parental awareness of risks faced by youth.7 Yet, despite this remarkable progress, researchers continued to highlight evidence of problems encountered by young people.

More recently, the focus on protection in online safety has been augmented by a new policy direction introduced by the European Commission in its communication on The European Strategy for a Better Internet for Children (or ‘better internet’ for kids strategy).8 The strategy retains a commitment to self-regulation but with a new emphasis on promoting high quality, positive online content for children and placing a new responsibility on member states to support teaching of online safety in schools, raise public awareness and follow through with better implementation of safer internet initiatives developed at the European level.

**Time to Question our Efforts**

Following a decade and a half of sustained policy activity, it is timely to ask just what outcomes this policy investment has yielded. Has the combined series of European initiatives contributed to a safer or better internet? Are children better equipped and empowered in their everyday use of online technologies? Is policy keeping pace with a fast-evolving technology sector with new products and services creating new kinds of opportunities but also risks for their many young early adopters? Do stakeholders contribute equally to policy and are their contributions relevant? Just how important is child online safety when balanced against other considerations such as intellectual property rights, the digital economy, national autonomy and cultural differences in youth protection policy? The Safer Internet Programme has had a demonstrable impact on the safer internet landscape as evidenced by the pan-European network of hotlines...
INTRODUCTION

and awareness centres (European Commission 2006, 2008; Mathonnet and Badouin 2006). Its influence has also been felt through the manner in which it has fostered multi-stakeholder dialogue and cooperation. But with the planned expiry of the current programme at the end of 2013 and its post-2014 subject to a new European Commission mandate, a turning point for safer internet policy is inevitable. The following are some of the themes that are likely to feature in determining how safer internet policy should evolve in the future.

Since its inception, European policy has been characterised by an unshakeable commitment to self-regulation in the sense that industry has been recognised as the best qualified to identify and lead in the formulation of responses needed to protect young people. As argued by Vice-President Kroes: “regulation – rigid laws coming from Brussels – is not necessarily the right way forward. Self-regulation by the industry can develop tools that are produced more quickly; that react more flexibly given the fast-moving technological environment; and that more effectively achieve the goal of protecting and empowering children online” (Kroes 2011). Yet, as we argue in chapter 4 (this volume), self-regulation has involved a significant degree of input on the part of legislators and may more accurately be described as co-regulation or managed self-governance involving other stakeholders apart from industry. Safer internet policies have included self-regulatory processes alongside a series of other interventions and practices – including investment in infrastructure, research, education and policy oversight. Future safer internet policy may adjust the balance between such elements – self-regulation in combination with more directly interventionist measures – the implications of which it is crucially important that researchers assess.

Secondly, multi-stakeholder involvement has been a valuable and important characteristic of safer internet policy to date. The shared nature of the responsibility for online child safety has been recognised since the early days of the Safer Internet Programme. Parents were identified early on as crucial to the success of efforts to promote greater safety awareness (see chapter 11); NGOs (chapter 9) and educators (chapter 10) have also played central roles in delivering and supporting programmes, but with perhaps limited effect (see chapter 3). More pointedly, children themselves were often absent from early thinking on policy initiatives though more appropriately children are now seen as not just targets but also active agents in the policy making process (chapter 12). However, it remains the case that some of the central policy initiatives such as the CEO Coalition to make the internet a better place for kids are primarily targeted at industry and have limited scope for involvement by other interested groups. Can better mechanisms be found to facilitate contributions of other stakeholders? In particular, in keeping with the principles of children’s rights and enabling children to have a say in matters that affect them, can meaningful ways be found to incorporate their views that go beyond tokenism and are
practical as well as effective? Underpinning the commitment to multi-stakeholder involvement are important principles of accountability and transparency which, much like other aspects of internet governance, have come under renewed international pressure as governments worldwide seek to manage the expansion of the internet.

The role that research plays in informing internet safety policy is particularly important (see chapter 5). Early phases of the Safer Internet Programme did not include provision for supporting research – that was the remit of the Framework Programmes. However, the critical nature of the issues concerned and the lack of a reliable body of evidence on which to base policy meant that research has assumed an increasingly prominent role in policy-making. Funding new research – under the term “knowledge enhancement” – has been an integral part of the Safer Internet Programme since 2006 and has supported the creation of a knowledge base about children’s uses of the internet, psychological and sociological aspects of online-related child sexual abuse, and the implications for young people of convergence and emerging technologies. In addition to the EU Kids Online project, the Safer Internet Programme has funded research into inter alia internet addiction among young people in Europe (EU Net ADB), the behaviour of sexual offenders (POG – the European Online Grooming Project), and online processes of abuse (ROBERT – Risktaking Online Behaviour – Empowerment through Research and Training). From 2014, it is proposed that all such research activities will be incorporated within the Horizon 2020 programme, the primary funding programme for research and innovation within Europe, while the programmatic elements such as support for hotlines and safer internet centres will be part of the Connecting Europe Facility. Will such shifts undermine the close linkage between policy and research and hamper efforts to make policy more responsive to changes in the environment? For instance, could research findings such as identifying the harm caused by online bullying (Görzig 2011), or the fact that parents really do not know what their children are doing online (Staksrud 2005; Livingstone, Haddon et al. 2011) be possible without a dedicated knowledge enhancement programme on internet risks and safety?

The broader political environment within which safer internet policies are developed and deployed is also of crucial significance. Governments at national level as well as European parliamentary processes have been largely supportive of a ‘light touch’, self-regulatory regime, allowing major technology companies to operate freely across the single market with few restrictions. The Digital Agenda for Europe is the overarching strategy to drive Europe’s flagging economy through technological innovation and growth, prioritising faster broadband, wider-take up of digital opportunities, use of e-government services and investment in research. Corporate social responsibility combined with pressure applied at European Commission level has ensured that online
safety has remained a high priority for industry (see chapter 8). Yet the political impetus to maintain a balance between management of risks through coordination and oversight of regulatory processes and the need to drive economic growth through expansion of digital opportunities is one that may be more difficult to sustain as governments come under pressure to deliver results and maintain competitive advantage. Maintaining a regulatory oversight whether that is at the level of member states through the involvement of national regulatory authorities (chapter 7) or through wider, European supervision and evaluation of self-regulatory schemes (chapters 4 and 6) can be expensive and time consuming. More attractive from a regulatory point of view is the notion of a more digitally literate population, better equipped to deal with risks, with fewer problems and less need for regulatory intervention or complex rules. Protection of minors, special needs users and vulnerable populations therefore becomes a more specialised area of public policy, allowing resources to be targeted to those groups and their carers to ensure that they have the knowledge to protect themselves and access to technical resources to assist in dealing with problems as they arise on an individual level, in the lives of real people (chapter 3).

Policy Pillars, Players and Paradoxes
The various contributions in this volume address this large and complex area by focusing on some of the key assumptions, respective contributions and the on-going dilemmas within the field of internet safety. As we discuss in the foregoing, internet safety has been founded on a number of policy pillars, the subject of Part 1 of this volume, and around which the architecture of online youth protection has been constructed. These policy pillars include first of all a concerted effort to stem the flow of illegal content on the internet through self-regulatory systems such as internet hotlines (European Commission 1999). A second pillar of the approach has been to support users, parents and guardians in assuming greater responsibility for their children’s online use through the development of filtering and rating systems or schemes to identify and classify online content as a basis for safer internet use. Thirdly, awareness raising and educational efforts have been promoted to make users, parents, guardians and children more aware of the potential benefits of the internet and its downsides. Contributors take as their starting point the principal points of reference (content classification and filtering, awareness raising and hotlines to combat illegal content) in order to assess the rationale for policy initiatives and their respective outcomes since the first programmes were launched in 1999. The legislative and regulatory framework within which internet safety policies have been implemented is examined alongside assessment of some of the principal examples of self-regulation in the field.
INTRODUCTION

It has long been recognised that to be effective, internet safety has to be a shared responsibility. Hence, multi-stakeholder participation and engagement has created opportunities for different players in the policy process. The scale of engagement on the part of government, industry, civil society and users, both adults and youth, and the effectiveness of their cooperation in creating better policy is the subject of Part 2 of this volume. Here, contributors consider specific examples of policy development from the diverse perspectives of different actors in the policy process. In the transition from old to new media, for instance, a quite changed role for the media regulator has been envisaged highlighting the evolving nature of regulation in this field. Similarly, for companies, corporate social responsibility as much as regulatory compliance features in their approach to implementing safer policies and practices. The changed nature of responsibility for managing risks in the online world is, of course, felt most keenly by parents and by children themselves, the nature of which is considered in separate chapters. Education and civil society in the form of the numerous organisations with specialised interests in child safety and welfare have also been central actors in the formulation of policy, mobilising opinion and in delivering safer internet programmes.

Part 3, Policy Paradoxes, assesses ongoing dilemmas faced by researchers and others in contributing to policy development with variable experiences of how and when research supports policy outcomes. Policy themes straddle a number of competing objectives, such as balancing children’s rights for protection with participation in the online world; dilemmas faced by parents in mediating children’s internet use; and whether it is better to focus on harm rather than seek to manage all the risks encountered in the online world. The cultural context of risk and the very diverse European landscape within which policy operates adds further to the complexity of developing an effective, harmonised approach across the continent. Finally, we consider the increasing recognition given to a child rights-based approach in articulating policy and guidelines for promoting and protecting children’s welfare online.

Policy in areas of major public interest such as children’s use of the internet may be either reactive or proactive, responding to issues as they arise or more-future orientated in their approach (Torjman 2005). In either case, it is a decision-making process that requires careful assessment of the desired objectives and the optimal strategies towards reaching those goals. The aim of the research represented in this volume is to support good decision-making through the provision of timely and reliable evidence and to foster wider public debate about the effectiveness of decisions taken to date and options available for the future.
Notes

1. EU Kids Online is a multi-national thematic network which aims to stimulate and coordinate investigation into children's online uses, activities, risks and safety, funded by the EC Safer Internet Programme. Between 2009-2011, EU Kids Online II designed and conducted a major quantitative survey of 9-16 year olds experiences of online risk in 25 European countries. For more information, see www.eukidsonline.net.


6. See the dedicated website for Safer Internet Day at http://www.saferinternetday.org/ See also the European Commission site: http://ec.europa.eu/information_society/activities/sip/events/day/index_en.htm


9. The CEO Coalition of leading technology and internet companies was established in December 2011 to make the internet a better place for kids. Following an invitation by Vice-President Kroes, 31 companies agreed a Statement of Purpose and a 12-month plan of actions in 5 main areas: simple and robust reporting tools; age-appropriate privacy settings; wider use of content classification; wider availability and use of parental controls; and effective takedown of child abuse material. http://ec.europa.eu/information_society/activities/sip/self_reg/index_en.htm


References


INTRODUCTION


Part I
Policy Pillars
Chapter 1

Filtering & Content Classification

Elisabeth Staksrud & Jørgen Kirksæther

On December 1st 2011, Commissioner Neelie Kroes, Vice-President of the European Commission and responsible for Europe’s “Digital Agenda”, called upon Internet industry stakeholders to specifically concentrate on a “wider use of content classification” and “[a] wider availability and use of parental control tools” in order to deliver a better Internet for kids (Kroes 2011).

The initiative, accompanied by an industry coalition (Coalition to make the Internet a better place for kids, 2011) rejuvenated an old – and by some presumed settled – debate on using technical tools in general and content classification and filtering services in particular, to protect European children from online content. Why were these ideas re-launched? What had changed? Anything? Given the controversial status of content filtering, its effectiveness and its implicit intrusion on an individual’s right to participation, expression, information and privacy, not to mention its inherent technical potential for political and commercial control, one needs to look at the arguments presented to understand the rationale behind its resurrection.

This chapter presents an overview of the European Commission’s history of supporting attempts to create systems for the classification of online content – and the subsequent potential for automated filtering of it, and discusses these in light of findings from the EU Kids Online project. The financial support and arguments are described and discussed, and comparison is made between the first attempts and the present situation. Finally, the chapter puts forward a recommendation, based on the above findings, previous experiences with the technology in question and the existing legal framework in Europe.

The EC Safer Internet Programme and Filtering1

In terms of practical policy implementation, the issue of online risk and safety for children has been the subject of initiatives across several different EU
programmes and bodies. However, within the European Union, including the countries in the European Economic Area (EEA), the question of children and potential online risk has found a common approach under the European Commission’s *Safer Internet Programme*. The programme, originating from the *Internet Action Plan* (1999-2004) (European Commission 1999-2002, 2003-2004), was extended into the *Safer Internet Plus Programme* (2005-2008) (European Commission 2005; European Parliament & European Council 2005), and found its current form under the *Safer Internet Programme* (2009-2013) (European Commission Information Society 2009; The European Parliament and the Council of the European Union 2008), see also table below. The approach to the development of these programmes was based on four basic policy principles (European Commission 1999-2002: 3):

1. The Internet is a positive instrument, empowering citizens and educators, lowering the barriers to the creation and distribution of content and offering universal access to ever richer sources of digital information. Whilst aiming at a high level of protection, any action taken to deal with atypical use for illegal and harmful content should not have a disproportionate impact on Internet users and industry as a whole.

2. Information on the Internet should be allowed the same free flow as paper-based information. Any restrictions should respect fundamental rights such as freedom of expression and the right to privacy.

3. Responsibility for prosecuting and punishing those responsible for illegal content remains with the national law-enforcement authorities, assisted by structures such as EUROPOL and INTERPOL.

4. Industry has a responsibility to remove illegal content from their systems, and can be assisted by self-regulatory bodies. Users should also be able to report illegal content to hotlines. Filtering software and rating systems can help users to avoid harmful content.

This chapter addresses principle 4, how filtering *developed* into practical policy, and examines some of the dilemmas associated with its use.

**What Is It?**

In principle, the *labelling* and *filtering* of content are intrinsically linked. The purpose of the categorisation of content (labelling it) is for it to be filtered – by *someone* – and the filtering is dependent on some sort of description attached to the content or its container/carrier. Both processes can be performed by automated systems, as well as by human intervention. The classic example of the latter is the work performed by various European film classification boards,
where films destined for cinema exhibition were pre-screened by a board of censors, and subsequently denied distribution or labelled with an age limit – in turn used by the theatres to restrict (or filter) admission. In recent years, this system has undergone major changes, not least in the transferral of the filtering process from the cinema to the child’s guardians. But, labelling remains as an indicator to be used by the filtering body, even if in several European countries it is no longer as a mandatory one and instead places the choice of heeding the label or not with the guardians.

Automated filtering (and labelling) works along similar lines, where a blocking mechanism reacts to a set of predefined rules, usually in the form of computerised algorithms combined with whatever the system can glean from the content itself or a content descriptor. The descriptor can be created by another automated system, by a human, or by a combination of the two. As an example, the Pan European Game Information (PEGI) system (see chapter 6, this volume) uses a set of predefined content descriptors chosen by the content’s creator.

Where the filtering system resides greatly impacts its capabilities, the potential uses to which it can be put, as well as the legal implications associated with it. If the system is fully self-contained (i.e. able to analyse content on its own), it can be placed anywhere, from a central distribution cluster to the end-user’s own equipment. If however, as with most systems, it needs to either rely on databases or updated rule-sets, it at least needs to access central server(s) regularly.

The core task of any automated labelling/filtering system is to do the job previously done by hand (and eye, training, opinion and experience) without the end consumer noticing its workings. In the following, the European Commission’s attempts to support the development of such systems are discussed.

The Early Years

From the outset, European policy on online safety had a strong emphasis on the development of technical tools that could aid parents and teachers in protecting children from potentially harmful and unwanted online content. The first Internet work programme (1999-2002) was allocated a funding of € 25 000 000 (European Parliament & the Council 1999: L 33/33 Article 31-33), of which action line 2 – developing filtering and rating systems – was given the highest allocation of funds of up to 38% of the total amount (European Commission 1999-2002: 3–4). In the follow-up to the programme, the European Parliament and the Council changed the expenditure to an indicative breakdown of 25-35% for fighting illegal content, 10–17% for tackling unwanted and harmful content (including filtering and content rating efforts), 8-12% for promoting a safer environment and 47–51% for awareness-raising efforts (European Parlia-
ment & the Council 2005, p. L 149/111 Annex II). While filtering and labelling strategies were discussed mostly during the first years of the Safer Internet Action Programme, the technical efforts of labelling and filtering still accounted for a quarter of all EC funding given to safety action lines for the first decade of practice (see Figure 1 below).

**Figure 1. Distribution of EC Funding on Online Safety Action Lines 1999-2008**

In the first work programme for the Safer Internet Action Plan (1999-2002), two technical solutions were strongly supported: projects that would *demonstrate the benefits of filtering and rating* and projects that could *facilitate international agreement on rating systems of online content* (DG Information Society European Commission 2001; European Commission 1999-2002). For the former, the objective was to encourage the establishment of European filtering and rating systems. For the latter, the objective was directly linked to a concern of Europe being left behind:

Work is already underway in a number of bodies dealing with protocols and with the design of a rating system to deal with the various requirements. It is essential that Europe’s voice be heard in international discussions and concertation meetings will be organized to ensure this. (European Commission 1999-2002: 11)

The wish for European filtering and classification tools was also part of a homogenization effort, trying to implement standard systems across the Member
States (such as PEGI, see chapter 6 this volume). For instance, in 2002 the European Commission commissioned a large study aiming (1) to identify the economic impact of ratings heterogeneity; and (2) to uncover any confusion that it may cause, particularly among parents, teachers, or others responsible for minors (see Olsberg|SPI & KEA European Affairs 2003). The report, however, concluded that there was neither industry nor consumer pressure for homogeneity, but that there was “structural pressure” towards uniformity pointing to technological changes and the “twin forces” of globalization and convergence (Olsberg|SPI & KEA European Affairs 2003: 16).

Commenting on the subsequent transformation of the Internet Action Plan into a multiannual programme, the European Economic and Social Committee (EESC) linked the development of positive content for children to the development of filtering tools, articulating a vision for

... an enlarged walled garden [that] could be created and moderated for children under a .kids.eu domain as envisaged in the "US [sic]. However it would have to be protected from paedophile activity and the need for more filtering and “notice and take down” on the rest of the Internet would remain, since children could not be expected to be limited to such an area (they would want to visit museums etc. at least) and since adult views on taste and decency also require a response (European Economic and Social Committee 2002: 5)

The focus on filtering and rating efforts by the EC was controversial and generated criticism from both children’s rights advocates, regulatory authorities and industry stakeholders (Electronic Privacy Information Centre 1999; Staksrud 2002), as well as concern from academics (Oswell 1999; Price 2002). It also garnered strong appraisal and academic support (see, for instance, Waltermann & Machill 2000). While recognizing the two main criticisms, that filtering does not work and that it has a chilling effect on free speech, the EU view was, as phrased by the European Commission, that (1) filtering is a form of user empowerment; (2) filtering is a parental choice; and (3) filtering tools should meet the individual requirements of European users (DG Information Society European Commission 2001). With respect to the latter, the then EC Commissioner for Enterprise and Information Society, Erkki Liikanen, emphasized that parents and teachers should have the means to “filter according to their value judgments” and that cultural and linguistic differences should be taken into account (Liikanen 2000).

The types of filtering discussed were typically based on one or more of the following principles:

- Blocking of defined files/sites (e.g. websites or newsgroups) by comparing URLs, names or the IP address of objects with a list of forbidden sites (“blacklisting”/“redlisting”)
• Blocking of all Internet content files/sites, except preapproved files/sites ("whitelisting"/"greenlisting")

• Filtering of selected files by assessment of the content of the files vs. pre-defined categories – such as particular words/combination of words, percentage of colour defined as skin-tone etc.

• Filtering of selected files by comparing a classification label embedded in the file/site with a pre-defined set of classification criteria.

The filtering itself could then be implemented on the desired level: on an individual computer, on the server or on a national level using proxy servers (Staksrud 2002).

ICRA & RSACI

Wishing to develop a comprehensive European system for the labelling and classification of online content, the European Commission strongly endorsed\(^8\) the adoption of the RSACi-system (Recreational Software Advisory Council on the Internet) from the ICRA (Internet Content and Rating Association). The expectation was that a working system “…would establish a direct communication channel from the content provider to the parent with no intermediary to control the flow of information unless the parent themselves chose to use a third party filtering template” (Archer 2009: 5).

Technically the system was based on the labelling of online content by filling out an online questionnaire. This would generate a code that was to be embedded in the metatext on the website in question. This code would then be read by different filters, that would block or allow the site to be displayed, depending on the level of restriction chosen (or censorship as it was labelled in the browser) by the user installing the filter, whether it be a government, a church, a school, or a parent. Typically a code would look like this:

http://www.rsac.org/ratingsv01.html l gen true r (n 0 s 0 v 0 l 0)

The example above is taken from the Disney site, and shows that the site (at the time) did not contain any nudity (n 0), sex (s O), violence (v 0) or obscene language (l 0).

The RSACi system originated in the United States after Senators Lieberman and Kohl in 1994 introduced legislation to create a government-run ratings board for computer and video games, but at the same time gave industry one year to create a self-regulatory scheme. By the summer of 1994, the US Software Publishers Association and five other US trade associations came together to create the RSACi content rating system (ICRA 2000). The system, gradually also adopted for online content, was based on the idea that Internet services and
content providers, as well as independent third parties and industry organizations, would classify and label Internet content (websites) by assessing it under the four categories of nudity, sex, violence and bad language. Generally, the labelling of online content was seen as the least intrusive system of parental control “while protecting freedom of expression” (Balkam 2001). The ICRA organization, defining itself as an independent, non-commercial organization, was owned by key industry actors such as Microsoft, IBM, America Online, Bertelsmann Foundation, Cable & Wireless, Deutsche Telecom Online Service and the Japanese Electronic Network Consortium (see Staksrud 2002: 77-89 for a detailed account of the system and the stakeholders behind it). Thus, the system was embedded in key software such as the Internet Explorer (from 1996) and Netscape Navigator (from 1998) browsers. In 1997, IBM also implemented the system on their proxy servers (Staksrud 2002: 80). In addition, the system received support from leading companies within the online adult entertainment industry, most notably the Adult Chamber of Commerce, Adult Entertainment Broadcast Network, Larry Flynt Productions and Playboy Enterprises Inc. (AVN Online 2002).

The promise of the ICRA system was such that the EESC advocated that Internet content providers who did not rate their content with the RSACi system using the ICRA standard should be “frozen out of the market”. Thus, the EESC wanted all computers sold to have child-safety software pre-installed, and set to the highest security level by default (European Economic and Social Committee 2001: 8). ICRA also had the ambition to make the system applicable to all media platforms, formulating proposals early on for how its system could replace national movie ratings systems (ICRA 2001). In addition, the filter was intended to be a global solution (Staksrud 2002).

Some fundamental flaws of the ICRA system were apparent. One of the most critical was the issue of providing neutral content descriptors. While the concept of “risk” in relation to children and media is culturally and individually framed (see chapter 3, this volume), a global classification system allowing for cultural, political, legal and individual preferences requires that the descriptions of content are in fact descriptive, factual and without normative judgements. However, describing content and assessing it as “pornography” or “violence” is a challenging exercise. The industry stakeholders behind the RSACi system, who made up ICRA, argued strongly that the descriptors used to formulate the questionnaires were in fact “value-neutral” and “because all templates will be based on a common language, end-users (or other organizations) can mix and match them to produce custom templates suitable to their ideological tastes” (Waltermann & Machill 2000: 43).

The ICRA system did not deliver as expected, and by 2011 it was discontinued (Family Online Safety Institute 2010). In addition to the reasons outlined above, the ICRA approach was hampered, opposed and hamstrung by a range of issues,
from flaws, political opposition and NGO pressure, to clashes with a changing Internet and online environment. As outlined by chief technical officer Phil Archer in his 2009 account of the problems experienced, the main application envisaged was in fact not by parents but the office environment, where employers might use it to filter out non-work content. Archer’s argument, based on his experiences within the filtering industry, is that filtering tools are very rarely bought by parents, even giving them away has not worked. The main argument, however, is that “[l]abel-based filtering can only work when a critical mass of sites is labelled.” According to Archer, “[m]ost of ICRA’s own members never labelled their site” and so the demise of the system was inevitable. (Archer 2009: 23).

In addition to the ICRA system, the EC has also endorsed other efforts, such as the “World Wide Web Safe Surfing Project (3W3S)” (2001) (Thales Communications 2003; Webwasher 2001). 3W3S consisted of six partners, from industry and from the academic sector. Its main purpose was to develop the Webwasher filtering system (now a part of McAfee’s server products, known as McAfee Web Gateway). This system was different to the ICRA system in that it was to “... immediately filter the vast amount of online material created every day, based on a central rating team and computer-aided techniques”. Webwasher never gained any foothold with consumers, and was eventually bought out by McAfee and included as a part of their business-/server-oriented packages (McAfee 2009). (As a side note one may add that several web articles exist for instance, on youth activist sites, outlining how to bypass the surf-wall by using a proxy.)

The Second Round

ICRA and its siblings never gained any widespread foothold – as already described, for good reasons. Yet, in her blog/public communication channel, Vice-President Kroes in November 2012 states “Protecting children is a priority for all of us. We are all aware of the risks that kids face online; we all want to avoid them; and we all want to do that without losing the many benefits of an open, innovative online world – benefits for the young and old.” (Kroes 2012). She continues: “After all, kids face risks in the “real world” too – like on the roads. We don’t ban them from going outside: rather, we equip them with the awareness and the tools to stay safe. We should do the same online too. So yesterday, we and the US underlined the importance of raising awareness, and helping parents and children make informed online choices. ... It’s time we had devices, content and services that are “child-safe”, so that adults can trust them, and leave their kids to explore and enjoy safely. [orig. emphasis]”

If this seems familiar, it’s because it is. Albeit suggested as one of several pillars of the on-going work on improving the online world, what stands out are the pointers towards the old ways: child-safe tools and areas. The Commis-
sion underlines this in its press release for the launch of the “Digital Agenda” (European Commission 2012):

Actions are grouped around four main goals:

- To stimulate the production of creative and educational online content for children and develop platforms which give access to age-appropriate content;
- To scale up awareness raising and teaching of online safety in all EU schools to develop children’s digital and media literacy and self-responsibility online;
- Creating a safe environment for children where parents and children are given the tools necessary for ensuring their protection online – such as easy-to-use mechanisms to report harmful content and conduct online, transparent default age-appropriate privacy settings or user-friendly parental controls;
- Combating child sexual abuse material online by promoting research into, and use of, innovative technical solutions by police investigations.

Of particular interest here is the third point. Not only are filtering tools yet again being put forward, they are to be transparent and user-friendly. Combined with the explicit statement from Vice-President Kroes outlined above, this is, in effect, if not a new idea, then at least a new openness: the aim, then, is the formulation of technical measures so easy to use that they will allow parents to feel safe enough to leave their children to themselves while using online services.

The other new major push announced by the EC, is the inclusion of children’s rights in the discussion. Again from the press release: “February 2011, the Commission presented an EU agenda for reinforcing the rights of the child by putting the principles of the European Charter of Fundamental Rights into practice (IP/11/156). It includes a series of concrete actions where the EU can provide added value to policies for children’s well-being and safety, including promoting child-friendly justice, better informing children about their rights, and making the internet safer for kids.” Noteworthy is the emphasis on children’s rights, as opposed to civic and/or human rights. Whether the latter two are taken for granted or left out is unclear. This yet unanswered question is of interest, as there have been recent incidents where national courts have ordered ISPs to block and/or filter certain websites and networks due to copyright infringements while legal opinions suggest that such orders violate “European fundamental rights” (Anderson 2011). Implications for child-protection filtering vs. rights are yet to be clarified and leave ample room for further considerations of the policy pillar of technical control of online access and content.
If it Worked – Would We Want It Anyway?

There is no denying that technical filtering tools pose a form of restrictive mediation that seemingly allows parents to use a piece of technology for protection, rather than having to address the embarrassing challenge of talking to their children about sexual activity in general and pornography in particular. The principle also promises mediation by proxy – online safety ensured also when parents are not physically present when children are online.

As an immediate response to the EC initiative, and in order to inform policy, the EU Kids Online network published a short report to see if research evidence as collected in the EU Kids Online survey of 2010 supported the recommendations of the CEO Coalition for a better Internet for children. Looking at content classification the study found that in Europe one in three parents (33%) claims to filter their child’s Internet use and one in four (27%) uses monitoring software (Livingstone, Ólafsson, O’Neill, & Donoso 2012). Parents are more likely to use filtering if they are regular and/or confident users of the Internet themselves, if they are worried about online risks their child may face, or if their child is younger and/or less experienced in Internet use. Although it seems that the more filtering, the less online risk, this is because younger children encounter less risk since they use the Internet less, and are more subject to parental controls – and vice versa. The EU Kids project also emphasises how:

...EU Kids Online knows of no research on actual usage rates of filtering software, or assessments of its effectiveness, which have been derived from in-home observation by independent research. Although there is little research that clearly demonstrates positive impact of using parental controls on the safety of children online, other types of mediation – such as the active involvement of parents in their children’s Internet use – seem to have a more positive effect. (Livingstone et al. 2012: 20, original emphasis)

At the same time: just as with traditional discourses on children and risk – or media and risk – public discussion on what constitutes online risk is complex and culturally framed and has been so since the formative years of the public Internet. Cultural differences in general, and in relation to media and the Internet and the question of risk (and harm) in particular, have been well documented in existing studies. For instance, in an early comparative survey of attitudes towards online content and risk in Germany, Australia and the US (Köcher 2000), clear differences were found regarding what constituted unwanted content. For instance, it was found that 43% of the US population would “block by all means” pictures of nudity, while only 13% of the German population would do so. Also, 58% of the German population would block radical left- or right-wing opinions, while 26% of the US and (reportedly) none
of the Australian population would do the same. Even between seemingly homogenous cultures such as the Nordic countries, differences can be observed. The first SAFT survey (SAFT project 2004; Staksrud 2003; Staksrud 2005; SAFT Project 2004-2006), researching among other things the parental perception of online risk in four Nordic countries, found differences between parents in Denmark, Iceland, Norway and Sweden. These countries are in terms of international comparisons often perceived as a homogenous cultural group (and are all categorized under “the Nordic Welfare State Model” umbrella). Most striking is that, while the level of concern was greatest in relation to children’s potential access to pornography online, substantial national variations could be observed, where Danish parents stand out as the least concerned (15% vs. 24% in Norway, 29% in Sweden and 32% in Iceland). The number one concern for Danish parents was that the Internet was time consuming (23%, compared to 3% in Iceland).\(^{10}\) It should be noted that when asked if the benefits of the Internet for children were greater than its presumed negative aspects, 56% in total (and 72% of the Danish parents) strongly agreed, 30% of the parents somewhat agreed, and only 8% in total answered that they somewhat disagreed or strongly disagreed.\(^{11}\) While it is now almost a decade since this data was collected, more recent research from EU Kids Online shows that there are indeed differences (albeit not always extensive) to be observed between the Nordic countries, both in terms of parental mediation as well as children’s risk behaviour (Livingstone, Haddon, Görzig, and Ólafsson 2011; Lobe, Livingstone, Ólafsson, and Vodeb 2011).

In conclusion, one can say that it is difficult to conclude. So far, tools for the classification and filtering of online content have been unable to show any sign of success or effectiveness, and have repeatedly proved to lack effectiveness in general, especially for smaller language groups. As content in some way or form must be described and ranked, there is also the inevitable challenge of developing neutral content descriptors independent of cultural, normative, religious, political, gender-based (…etc…) connotations and perspectives. Software is designed by people. Automatic algorithms are defined by people. One must be able to describe and define, for example, pornography in an international environment. The US Supreme Court’s Justice Potter Stewart could only define it as “I know it when I see it” (quoted in Thornburgh, Lin, & National Research Council (U.S.) (Computer Science and Telecommunications Board, 2002: 21).

This is the same for blasphemy. For art. For gender issues. For all content. For us all, regardless of our cultural, ethnic or religious background.

And – should one get past this obstacle – there is the question of relevance. Are filtering and classification tools relevant? Are they the best and most efficient way to protect children? Are we opting for a technological quick-fix instead of starting down the tedious and sometimes embarrassing road of talking to children and educating them? And does this fix at all match the complex roles
and realities children enter into when out-and-about in the online sphere – as producers, consumers and participants of online content – and connecting with others and conducting themselves in various ways? Who is competent to take on this complex world and keep children safe? Parents? Maybe not, as findings from EU Kids show that overall, only a quarter of children (27%) and a third of parents think that parents are effective in helping to keep children safe online (Livingstone et al. 2012: 17). And, again, have we really clarified, debated, and accepted the rights-based implications of content classification and filtering? And who should the “we” be to do this? Are children themselves included?

There is a saying that the best, most robust and adaptable filter you can install is the one between your children’s ears. In the tension between protection, participation and fundamental rights this is at least something to do while we wait for rights-based relief.

Notes
1. This section builds upon and has been partly published in two previous publications (Staksrud 2002, 2013).
2. Most relevant here would be the Daphne Programme which led to the development of Hotlines (for more information, please refer to Chapter 2, this volume), the Fifth framework programme (where under the IST key action provisions were made to support the development of filtering technology), the Learning in the Information Society programme (where encouragement of the use of new technology and the interconnection between schools was central), and Promise (a five year Community programme aiming to stimulate the establishment of information society in Europe by increase public awareness and understanding of the potential impact of information society across Europe) (European Commission, 1999-2002 Annex 1).
3. Albeit not members of the European Union, Norway and Iceland are members of the Safer Internet Programme through the European Economic Area cooperation. As such they have contributed financially to the programme since September 24th 1999, after the EEA decided to change protocol 31 in the EEA agreement to include cooperation on particular areas outside the ones defined under “the four freedoms”. See Staksrud (2002: 70-71) for more details. It should also be noted that the author was the Norwegian representative in the IAP programme committee (reviewing the EC’s work on the Action Plan), 2000– 2001.
4. It should be noted (in the interest of reflexivity) that Staksrud in her professional capacity has received project funding from all these programmes, specifically the SAFT project (2002-2004) under the Safer Internet Action Plan, the NONO (2004-2006) and AWAREU (2004-2006) projects under the Safer Internet Plus Programme, and participated in the EU Kids Online project (2006-2009), EU Kids Online II (2009-2011), and the EU Kids Online III project (2011-2014) under the Safer Internet Programme. In addition, Staksrud has conducted various reviews for the European Commission’s Safer Internet Action Plan, most a notably review of all EC funded hotlines (2001), the 2006 Safer Internet part of the Eurobarometer (Eurobarometer, 2006) and the independent assessment of the Safer Social Networking Principles (See Lobe and Staksrud 2010; Staksrud and Lobe 2010 for the assessment reports).
5. For a complete list of previously funded filtering and labelling projects, see Safer Internet Programme (2013).
6. Figure generated from various research and evaluation reports on and from completed EC funded projects, see http://ec.europa.eu/information_society/activities/sip/projects/completed/index_en.htm for overviews. Reliable data could not be obtained for projects not completed by the time of writing. In addition to this comes support for other initiatives, such
as self-regulation schemes, where the EC does not provide project funding, but rather hosts industry and stakeholder meetings and conducts independent evaluations and other similar supporting activities. The figure was originally published in Staksrud (2011: 135).

7. The European Economic and Social Committee (EESC) is a consultative body that gives representatives of Europe’s socio-occupational interest groups, and others, a formal platform to express their points of views on EU issues. Its opinions are forwarded to the larger institutions – the Council, the Commission and the European Parliament. It thus has a key role to play in the Union’s decision-making process (EESC, 2010). See http://www.eesc.europa.eu for more information.


9. National as well as regional and local patterns of risk perceptions have been demonstrated by other types of research, see Zinn & Taylor-Gooby (2006: 30-31) for a short overview.

10. The results also showed significant variations in parental concern pending on the gender of the child they were thinking of when answering the questionnaire. The total selection showed that parents of boys were significantly more concerned over pornographic sites (27% vs. 20% of parents of girls) and time consumption (13% vs. 9% of parents with girls), while parents of girls were significantly more concerned over the risk of meeting strangers/dangerous people (15% vs. 6% of parents of boys).

11. Similarly, in the UK in 2003, 59% of the respondents in the national Oxford Internet Survey said that they supported the continued diffusion of Internet despite the general awareness of potential risks (Dutton & Shepherd 2005).

References


Chapter 2

Internet Hotlines

_A Reporting Solution for Internet Safety?_

Brian O’Neill

The shadow of online child sexual abuse material presents one of the most
notorious downsides of the internet and is something that has long preoccupied
governments, the internet industry and child welfare organisations. Around 1995,
law enforcement agencies and child protection specialists became concerned
about the ease with which the internet could be used to propagate extreme
harmful content, such as child sexual abuse material\(^1\) as well as extreme forms of
racism and hate speech. Where previously such material was relatively isolated
and rare, the internet appeared to make it easier to produce and distribute illegal
sexual images in a new medium, apparently without regulation or censorship.
Worryingly, the internet also provided new opportunities for abusers to access
and make contact with children and young people online (United Nations 2009;
UNICEF 2011). An early response to this threat was the establishment of internet
hotlines for the reporting of illegal content, a pragmatic response to the lack
of law enforcement expertise which found itself ill-equipped to deal with this
new form of cybercrime (Carr 2012). Hotlines sought to strengthen policing
of the internet through cooperation between law enforcement, industry, civil
society and the general public (Chen 2010). Along with filtering/content clas-
sification and awareness-raising, hotlines quickly became central to the fight
against illegal content online and a cornerstone of the first Safer Internet Action
Plan of the European Union (European Commission 1999).

The central idea of an internet hotline is to allow users to anonymously
report content they may come across which they suspect to be illegal. Reports
are acted upon by trained analysts and notified to the police and internet service
providers for action. This may include taking down the material at source and/
or initiating a criminal investigation. Hotlines are nationally-based and subject
to local legislation and agreements governing the scope of their remit. The fight
against child sexual abuse material on the internet, however, is an international
one. INHOPE, the International Association of Internet Hotlines, with support
from the European Commission, acts as the principal network facilitating coop-
eration between hotlines for the purpose of ensuring a faster and more efficient response to complaints about illegal content across borders.

This chapter discusses internet hotlines in the context of overall strategy to make the internet a safer place for children. As a bottom-up, self-regulatory initiative, do hotlines make the internet safer? Or do they merely touch the surface of the enormous problem of illegal child abuse content on the internet? From the perspective of child protection, the circulation of such material is of paramount concern, and necessitates action at the highest inter-governmental level to combat what is almost universally regarded as an abhorrent crime. Hotlines have been part of the solution, instigated by and supported by industry and child welfare groups since their inception. Hotlines also gain substantial public financial support through participation in national Awareness Centres, most of whom are part-funded by the European Commission, and in lieu of more direct state or regulatory intervention, have been a prominent example of combined efforts to tackle one of the most unsavoury aspects of the online world. But if it is the case that, far from disappearing, the problem of online child sex abuse grows ever more serious, what other options are available to policy makers in dealing with this challenging area?

The European Regulatory Framework

As early as the mid-1980s, legislators in the course of the drafting of the Television without Frontiers Directive (1989) recognised the problem of harmful and illegal content as a matter of major political importance. The European Commission signalled that it would introduce proposals to protect minors and human dignity in the context of new audiovisual services. Once published, the Green Paper (European Commission 1996) emphasised the need to enforce existing legislation and criminal laws while encouraging industry to monitor itself, such as by a ‘self-regulatory body set up to identify illegal content or from an equivalent body in another country’ (European Commission 1996).

Recommendation 98/560/EC (Council of the European Union 1998), promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity, advocated the creation of “hotlines” in order “to promote the effective management of complaints about content which does not comply with the rules on the protection of minors and/or violates the code of conduct.”

In 1999, the European Union adopted its first multi-annual Action Plan for a Safer Internet, framed by the twin objectives of promoting a safer internet environment for all consumers and combating harmful and illegal uses of the internet, in particular ‘offences against children and trafficking in human beings or for the dissemination of racist and xenophobic ideas’ (European Union 1999).
In promulgating the idea of hotlines, the model of a self-policing network of users was supported, building on the community ethos of the internet itself, and seeking to harness the capacity of concerned users and members of the general public to monitor online content (Huey, Nhan et al. 2013).

Internet service providers (ISPs), as the organisations who provide access to the internet, played a key role in developing the concept and functional organisation of hotlines as a response mechanism. Under the E-Commerce Directive (Council of the European Union 2000), ISPs, typically, do not have legal liability for content carried on their networks for which they act as a mere conduit providing access to the internet. With regard to caching and hosting of third party content, ISPs are exempted from liability once they take reasonable steps to take down or block access to content that has been identified to them as illegal in the form of so called ‘Notice and Take Down’ (NTD) provisions. Systems for ‘notice and take down’ have become the primary mechanism by which internet service providers comply with the requirements of the E-Commerce Directive (Van Eijk, Van Engers et al. 2011). In return for protection from liability, industry providers undertake to remove illegal content once duly notified. Hotlines operate primarily on the basis of such a ‘notice and take down’ system, acting as the reference body for processing notifications of suspected illegal content. The INHOPE network of hotlines ensures that on an international level its members comply with NTD requests and that prompt action is taken once notification is received. Complications arise, however, due to the different legal systems applying in different countries. The very heterogeneous way in which hotlines interact with law enforcement prompted the Commission to urge Member States to take immediate action on harmonising standards with regard to criminal content and to promote a high level of international cooperation and exchange of information to combat the circulation of illegal content. Directive 2011/92/EU on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography (European Union 2011) achieves this to some extent and is discussed further below.

The Development of Internet Hotlines

The first internet hotline was established in the Netherlands in 1996 by the internet industry with the support of the police, followed shortly after by the Internet Watch Foundation (IWF) in the UK (Williams 1999). The Bertelsmann Foundation in Germany meanwhile developed the prototype for the processing and management of reports received from the public in its ‘contents concern response system’ (Burkert 2000). Hotline services also developed around this time in Norway (Redd Barna/Save the Children), the Netherlands (Meldpunt),...
Germany (Newswatch, FSM and Jugendschutz), as well as hotlines provided by internet service provider associations in Austria and in Ireland.

Internationally, Cybertipline, endorsed by the National Centre for Missing and Exploited Children (NCMEC), began operating in the United States with federal government support in 1998 (Detrick 1998). In 1999, a UNESCO Expert Meeting in Paris recommended the creation of a network of hotlines to serve as a kind of international “watchtower” to guard against the growing problem of child sexual abuse and exploitation on the Internet (UNESCO 1999). Childnet International, an NGO based in London, created a forum in 1999 (“International Hotline Providers in Europe Forum”) for hotlines to meet and exchange information. This initiative, with support from the EC Daphne programme, laid the foundation for an international network for information exchange, culminating in the establishment of the INHOPE Association in 1999, now representing 44 Hotlines in 38 countries across the globe (Insafe-INHOPE 2012).

European policy sought to integrate hotlines with other safety initiatives supported under the Safer Internet Programme (European Commission 2006) in order to ensure their greater visibility. Awareness nodes, set up originally as part of the SAFT project, became the basis for a wide scale public education and media awareness campaign (Staksrud 2005). Efforts were made to build greater levels of integration between the diverse initiatives so that in 2007, the establishment of integrated safer internet nodes (awareness node, hotline and helpline) was further encouraged under European funding programmes. It was recommended that each centre should have a single advisory board comprising relevant national stakeholders to exchange information about their respective activities, and agree ‘common positions on Safer Internet issues for submission to policy-makers and the media’ (European Commission 2007).

Hotlines, at least in the European context, are reliant for support on European co-funding. The question arises as to how many would exist without European support. Under the five-year Safer Internet programme (2009-2013), funding is provided for nationally-based Awareness Centres, for INHOPE and support for cooperation with other countries including Russia in the fight against illegal online content. Building on ten years of investment in this infrastructure, the policy emphasis is now on integrating national initiatives under the umbrella of Safer Internet Centres (SICs), comprising hotlines for reporting illegal content, and helplines where parents and children can obtain advice on how to deal with harmful contact (grooming), harmful conduct (cyberbullying), harmful content and uncomfortable or scary experiences when using online technologies (European Commission 2009). In this way, it is intended that hotlines, rather than standalone initiatives, are integrated as part of a Europe-wide service infrastructure that enhances user confidence and trust in the safety and security of the internet. Into the future, it is envisaged that hotlines will continue to be part of the safer internet service infrastructure under the Connecting Europe...
INTERNET HOTLINES

Facility, part of the Europe 2020 strategy which makes digital infrastructures a key driver in European policy (European Commission 2012).

Hotlines: Function and Operation

Hotlines vary in composition and in the scope of their operation. Looking to the 30 countries represented within Insafe, the European network of Awareness Centres (Figure 1), the national hotline in 12 out of the 30 countries (41%) is maintained by an NGO; in 5 countries (17%), it is led by an industry association; in 4 countries (14%) it is the government or a governmental agency that takes the lead; in a quarter of cases (7 countries), a consortium of industry, NGO and/or government agency organises and maintains the hotline. Only in the case of Norway, is it entirely managed by a law enforcement or police agency.

Figure 1. Hotlines within European Awareness Centres (Insafe)

Source: Insafe-INHOPE 2013.

Updating Williams (1999), Table 1 compares public and private sector involvement, illustrating some of the diversity of organisation types involved:
### Table 1.

<table>
<thead>
<tr>
<th>Type of Organisation</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Public Organisation</strong></td>
<td></td>
</tr>
<tr>
<td>Law enforcement agency</td>
<td>• Norwegian Criminal Investigation Service (Kripos) (NCIS)</td>
</tr>
<tr>
<td>Other wholly publicly owned body</td>
<td>• Jugendschutz.net, an agency set up by the German Länder responds to reports about illegal content</td>
</tr>
<tr>
<td>Publicly funded body</td>
<td>• RRT (Lithuania) an independent national regulatory authority for communications and the postal sector in Lithuania.</td>
</tr>
<tr>
<td><strong>Private sector/industry</strong></td>
<td></td>
</tr>
<tr>
<td>Run by Association</td>
<td>• AFA in France, FSM &amp; eco in Germany, ISPA in Austria, ISPAI in Ireland</td>
</tr>
<tr>
<td>Run independently with industry funding</td>
<td>• IWF in the UK is funded by the Internet industry but has non industry representatives on its board</td>
</tr>
<tr>
<td>Child welfare organization</td>
<td>• Save the Children in Iceland, and Denmark.</td>
</tr>
<tr>
<td>Other private organisation</td>
<td>• Meldpunt in Holland is a non profit “stiftung” with support from users, industry and Government</td>
</tr>
</tbody>
</table>

Note: Adapted from Williams (1999).

All hotlines receive and process reports of child abuse images on the internet, some also process reports related to other forms of illegal and/or harmful content such as denial of Nazi crimes (Austria, Germany), racism, xenophobia, self-harm (Czech Republic and others); some also provide technical advice and assistance in relation to concerns about illegal and harmful content (Internet Watch Foundation in the UK). Most also deal with all online media platforms including the world wide web, newsgroups and bulletin boards, Internet Relay Chat (IRC), instant messaging, email and social networking. While their primary responsibilities are to take appropriate action on reports received by relaying information to law enforcement and to issue notices for take down of offending content, some are also involved in education and awareness raising activities.

Typically, reporting mechanisms consist of an anonymous, online reporting facility. In some instances, other reporting forms such as telephone, email or fax are included. According to INHOPE guidelines, an online submission is designed to ensure that reports from the general public contain essential information for tracing and identifying suspected content and require reporters to accurately identify the location of the content, followed by a description of the suspect material using applicable legal categorisations (GSMA and INHOPE 2010). Internet
users are also encouraged to report other online content, such as peer-to-peer (P2P), UseNet, mobile apps or where spam email contains illegal content (child sex-abuse content, racist incitement) or links to such illegal content.

The standardised procedure for the processing of reports received by internet hotlines is outlined in Table 2.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>A report is received by the hotline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>It is assessed to see if it has already been reported and is in the system</td>
</tr>
<tr>
<td>Step 3</td>
<td>If not previously reported, it is assessed for possible illegality in that particular country</td>
</tr>
<tr>
<td>Step 4</td>
<td>If found to be potentially illegal and hosted in that country, agreed national procedures are followed such as reporting to law enforcement agencies and issuing a notice and take down order to the ISP</td>
</tr>
<tr>
<td>Step 5</td>
<td>If found to be potentially illegal and hosted in another country, it is cross-checked with INHOPE to see if any other reports already exist, and/or action is taken to notify law enforcement and issue a ‘notice and take down’ or to block to the relevant ISP.</td>
</tr>
</tbody>
</table>

Source: GSMA & INHOPE 2010.

The gathering of statistical data about reports received is another crucially important function of internet hotlines. Larger organisations such as the Internet Watch Foundation play an important role in analysing trends in child sexual abuse content online and where the content is hosted. Smaller organisations are limited to analysis of trends in reporting online illegal content within their country over time. INHOPE is in a unique position to compile such data, and has placed a large emphasis on its central report management system (INHOPE 2007). However, legal restrictions on data sharing in some countries has resulted in inconsistencies in reporting and has hampered efforts to create a comprehensive picture of the distribution of child sexual abuse material (Carr 2012).

Quantifying Illegal Content on the Internet

Hotlines process reports on suspected illegal content found online, notify relevant law enforcement agencies and assist in its removal from the internet. The illegality of suspected child abuse content is ultimately a matter for determination by courts of law in the country in which it is found. Definitions of child abuse material are typically taken to include “any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes” (UN General Assembly 2000). The legal definition of ‘child’ may vary between one jurisdiction and another, however, the European Union has defined the age of
18 as the EU-wide baseline for participation in pornography. Internationally, efforts to harmonise legislation outlawing online or computer-facilitated child abuse are improving though there are still 51 countries that have no legislation that specifically addresses child pornography (ICMEC 2013). Racism, xenophobia, threats of violence against individuals, financial scams and grooming for the purposes of sexual abuse also receive significant attention in the legal systems of most countries in the European Union (Cohen-Almagor 2013). In practice, however, most of the work undertaken by hotlines relates to reports of suspected child abuse material.

Child abuse did not, of course, begin with the internet; indeed, many child abuse images in circulation originated from pre-internet movies and magazines that have been recycled online (Quayle and Taylor 2003). Without doubt, however, the internet has greatly expanded the scale of the problem. Estimates of online child abuse material are difficult to determine, even unknowable (Teunissen 2012). The UN Special Rapporteur on the sale of children, child prostitution and child pornography reported that the number of sites devoted to child pornography had grown from 261,653 in 2001 to 480,000 in 2004. The number of predators connected to the Internet at any one time was estimated to be 750,000 (United Nations 2009). The number of individual images or video clips is estimated in the hundreds of thousands (Ainsaar and Loof 2011; Carr 2011). Through its international database, Interpol has succeeded in identifying approximately 2,025 children in child pornographic images. In 2012, INHOPE processed just over a million reports, 40% of which came from EU Member States (Insafe-INHOPE 2013). In 2010, the UK’s IWF processed a total of 48,702 reports, of which 30% contained child sexual abuse material (Internet Watch Foundation 2012).

The platforms used for the distribution of child abuse material online have also become more complex and sophisticated. In 2010, IWF identified a total of 715 unique commercial websites distributed around the world containing child sexual abuse material, underpinned by a complex network of hosting patterns, payment arrangements, advertising and registration systems (Internet Watch Foundation 2012). While child exploitation websites for commercial gain would appear to be in decline given the very great risks involved (European Financial Coalition 2010), distribution of child abuse material via web, email, newsgroups, chat services, ftp and peer-to-peer networking has expanded (Vettori 2007; Carr 2011). Even the social networking site Facebook has been found to have been used by paedophile rings to exchange child abuse content.5

The ready availability of ‘adult’ or legal online pornographic content has shaped the potential market and made both legal and illegal sexual material much more accessible to ordinary ‘viewers’ (Jones 1998; Moran 2010). Added to this is the ease with which new digital technologies facilitate ‘self-generated’ and ‘user-generated’ pornographic content, sometimes by young people them-
selves, leading to further complex issues for law makers and child welfare specialists (Leary 2010; Aiken 2011). The phenomenon of ‘sexting’ is accordingly having a bearing on the production and circulation of child abuse material in that sexually explicit images of minors can be produced by young people and can be further exploited for commercial or illegal purposes (Teunissen 2012).

How Effective are Hotlines?
Internet hotlines have been a prominent feature of the fight against illegal online content since the beginnings of the world wide web. But just how effective are they in combating use of the internet for propagation of child sexual abuse and other illegal material? This is a difficult question to answer and raises a number of issues, most notably, the availability of data with which to measure success; the extent of public visibility of hotlines themselves; as well as the question of filtering and blocking strategies that have been mooted as an alternative means of fighting illegal content.

Law Enforcement and Measuring Success
In both their legal framework and operational structure, hotlines act as intermediary communication channels between internet users and law enforcement on the basis that users are more likely to report illegal content if their anonymity is ensured, and if they do not have to deal directly with the police. Hotlines are described as acting in a support function or complementary role to national law enforcement:

Hotlines do not investigate offences or arrest or prosecute offenders. They .. represent centres of expertise regarding illegal material and sexual abuse of children in digital media, providing guidance to ISPs and other stakeholders as to what content might be illegal in a country. Close cooperation with the national law enforcement agencies is an important element of the hotline operation. (European Commission 2011)

Given their crucial relationship with law enforcement, a central issue is the minimum standard for organizations operating hotlines and the procedures to be followed in handling complaints (Vettori 2007). In 2003, the Safer Internet Action Plan observed that law enforcement agencies benefitted from the input of hotlines provided they were ‘official’ (recognized by Member States), had clear responsibilities and followed agreed protocols and procedures (European Commission 2003). Evaluation of the first phase of the Safer Internet Action Plan supported the claim that hotlines had been important in the fight against illegal content (Technopolis 2003). Concerns were raised, however, about the extent
to which hotlines encroached on the work of the police and the appropriate interface between reporting, investigation and collection of evidence for criminal prosecutions. In 2008, a further evaluation called for better cooperation with law enforcement as well as better feedback from police on the status of reports submitted (European Commission 2008). This, it was acknowledged, was not always feasible given the need to protect the integrity of investigations in progress.

If hotlines play a complementary and supporting role to that of law enforcement, how then can their contribution to combating illegal online content be evaluated? Quantifying the volume of illegal content, or providing indicators for the scale of the problem is inherently difficult, if not ultimately unknowable. Yet measures for success are needed if only to identify where to target resources. For hotlines and for INHOPE as coordinator, numbers of valid reports received provides the most important indicator (BDRC 2001). Hotline activity in processing reports has seen steady increase over the course of their operation, rising on average by approximately 20% per annum (INHOPE 2013). Between 2004 and 2006 a total of 1.9 million reports had been processed (INHOPE 2007). As a percentage of overall illegal content, 50% of reports related to child pornography. Data for 2012 reveals a total of 37,404 reports of child sexual abuse material were made across the INHOPE network, three quarters of which related to pre-pubescent victims (Insafe-INHOPE 2013).

Assessing such trends, INHOPE acknowledges, is difficult. Does the increased volume of hotline activity indicate success in terms of their impact and visibility, or simply point to the ever-increasing scale of the problem? Undoubtedly, there are increased rates of reporting due to more hotlines operating, better visibility and more accurate reporting of what is and what is not illegal content. But so too the population of internet users has increased, as has the volume of child abuse imagery in circulation.

From the perspective of law enforcement, one of the important functions that hotlines perform is providing a close link to industry and content hosting providers, predominantly within Europe but internationally as well. These are a key link between the content hosted online and end-users and are therefore pivotal for law enforcement (RAND Europe 2007). Close cooperation between hotlines, ISPs through representative organizations such as EuroISPA and law enforcement has contributed greatly to the minimizing of illegal content hosted within the European Union (Moran 2011). Thus, in pursuing actions on reports received and minimizing the delay in notice and take down, hotlines have been an effective tool in rapid response to web-based distribution.

However, there are inherent limitations to what a hotline can achieve beyond acting as a reporting mechanism and a communication channel between stakeholders. According to Interpol, hotlines are an element but not the sole solution to the core problem of global distribution of online child abuse imagery (Moran 2011). Ultimately, more powers of investigation and prosecution are
INTERNET HOTLINES

required in addition to firm government regulation and better policing resources to tackle the problem. Interpol argues that investigations are frequently hampered by poor access to technical data regarding hosting distribution of child abuse imagery, with the result that while obtaining the information necessary to process and investigate a report is *technically* possible, it is often *practically* extremely difficult (Moran 2011). Policing efforts have been targeted at greater international coordination of intelligence through the development of an International Child Sexual Exploitation image database and compiling information on the “worst of” sites distributing child abuse imagery. This has been used in conjunction with projects such as CIRCAMP to develop a filter that ISPs can use to block web domains disseminating child abuse imagery.

*Public Awareness and Impact of Hotlines*

The visibility of hotlines among users of the internet and the extent to which the general public is actually aware of what they do and how to use them is another area of concern (European Commission 2008).

Through successive phases of the Safer Internet Action programme, a high priority has been placed on promoting public awareness of hotlines and on the importance of their working alongside other initiatives in building awareness of safer internet use. Hence, the requirement within the Safer Internet Programme (2009-2013) that hotlines be part of integrated Safer Internet Centres within each Member State. Yet, consistent evaluations have found that public awareness of hotlines is exceptionally low. A review of the 1998 and 2006 Recommendation on the protection of minors and human dignity acknowledged that hotlines are ‘still not sufficiently known about by, and accessible to, Internet users and children’ (European Commission 2011). A Eurobarometer study carried out in 2004 found that just 5% of respondents identified hotlines as a mechanism to report illegal content on the internet. The most common answer supplied, not surprisingly, was the police, though 38% said they did not know where to report illegal or harmful content (Eurobarometer 2004). In 2005, awareness of where to report illegal content had increased – 47% said that they would report illegal content to the police – awareness of hotlines stood at just 4% (Eurobarometer 2005). Awareness varied substantially between countries with higher levels reported in Belgium (18%), the Netherlands (13%) and Austria (12%). In most EU countries, however, awareness was below 6%. Commenting on the first years of the implementation of hotlines, the Commission conceded that “while hotlines deliver a valuable service, the majority of Internet end-users have little or no knowledge about the existence of hotlines” (European Commission 2006).

By 2008, Eurobarometer reported that 38% of parents – when prompted – said they would report illegal content to a hotline. The vast majority of parents (92%) identified police when asked where, or to whom, they would report
illegal or harmful content seen on the internet. In some countries with high profile initiatives (Germany, Finland, Denmark, UK) awareness was high. But in the rest of Europe more than one-fifth of parents in Slovenia (27%), Bulgaria (25%), Spain (24%), Estonia (23%) and Poland (21%) were not aware that this was possible.

Findings from the EU Kids Online survey would also appear to support the general lack of awareness of online or industry-provided sources of information about online safety (Livingstone, Haddon et al. 2011). While the survey did not specifically ask about hotlines, parents and children were asked about sources of internet safety advice as well as which sources they would prefer to use. Most parents got their information from family and friends (48%) or from the mass media (32%). Just over a fifth of parents (22%) say they got information from internet service providers which would include information about national hotline services or websites with safety information (21%). When asked to choose their preferred source, parents identified schools (43%) and mass media (32%) as the most important. Online sources such as internet service providers (26%) and websites with safety information (24%) were chosen by about a quarter.

The relatively low impact that internet hotlines appear to have made on the general public prompts the more general question of who exactly they are aimed at? The notion of a hotline itself suggests a rapid response mechanism to which users can turn for immediate help and assistance as in the case of telephone support helplines offered by government or commercial industry services (Burkert 2000). Yet, this is not exactly what internet hotlines are set up to do. While offering a service to the general internet-using public, they do not as a rule provide feedback to users on the status of reports or provide wider advice on dealing with harmful content on the internet. INHOPE’s website, for instance, states that:

Due to the volume of reports received by Hotlines it is not always possible to update individual reporters. In addition, any reports that start a full police investigation will require confidentiality on behalf of the Hotline. Also as most reports received by Hotlines are anonymous it is in most cases not possible to advise the reporter.

Therefore, while nominally targeting the general internet-using public, in fact hotlines are more likely aimed at a smaller subset of users, such as users of adult pornography who may come across content they suspect to be illegal, as well as professionals such as administrators of computer networks who may come across suspicious content in the course of their work. Anonymous reporting of child sex abuse material, the handling and distribution of which is illegal throughout Europe, is therefore more likely to facilitate reports rather than going directly to the police. As such, the idea of an internet hotline is
INTERNET HOTLINES

probably closer to a confidential crime-reporting mechanism, which indeed it is. However, it does place awareness raising about hotlines in the difficult position of promoting a service that deals with one of the darkest aspects of the online world, and a subject matter that is likely to provoke wide scale public anxiety. Inviting reports, therefore, that involves users handling material of an illegal nature is something that is both challenging and problematic for awareness raising. Independence from the police and the assurance of anonymity may improve levels of reporting in such instances but requires a special legal status for third party organisations to handle such reports in the first place. It is also an obstacle to awareness raising efforts to promote positive aspects of the online world and instilling trust in the internet as a safe place.

Filtering and Blocking as Alternatives

Much attention has been given in recent policy debates to the potential for greater use of filtering and blocking known lists of sites containing child sexual abuse material as an additional strategy in combating the dissemination of illegal content online. Up to 2006, the European Commission had been largely neutral on the subject of blocking, with neither the Safer Internet Programme nor any of the principal legislative instruments involved – the E-Commerce Directive or the Recommendation on the Protection of Minors and Human Dignity – requiring or promoting blocking or filtering measures (McIntyre 2012). Indications of a new political impetus towards more direct governmental intervention in the fight against illegal content was evident in the debates that preceded the issuing of a new European Directive on combating the sexual abuse, sexual exploitation of children and child pornography (European Union 2011). Building on the declaration of the Czech Presidency adopting a new approach for a safer internet for children (the so-called Prague Declaration), broad political support was vouched for policing initiatives such as CIRCAMP and Interpol’s Child Abuse Image Database (ICAID) and formal acknowledgment that ‘blocking access to websites containing child sexual abuse material shows that this can be one very valuable component in the fight against child sexual abuse and exploitation’ (Council of Ministers of the European Union 2009, para 20).

While the blocking of identified child abuse websites, using blacklists derived from hotlines and Interpol’s ‘worst of’ websites, is a feature that has been deployed for many years in a number of European countries, especially in Scandinavian countries and the United Kingdom, it is something that has been strongly resisted by EuroISPA, the pan-European association of European Internet Services Providers Associations.

Law enforcement agencies strongly supported the adoption of mandatory blocking of child abuse sites in Directive 2011/92/EU on combating the sexual
abuse, sexual exploitation of children and child pornography (European Union 2011). This was subsequently amended in the final approved version, however, to a voluntary basis whereby Member States "may take measures to block access to web pages containing or disseminating child pornography towards the Internet users within their territory" (Article 25) noting the role of hotlines in strengthening policies to prevent sexual abuse and exploitation of children (preamble, paragraph 34).

While the Directive did not go as far as child safety advocates would have liked (Carr 2011), it is indicative of a greater emphasis on technological mechanisms to block access to illegal content within the European Union. Greater political support for blocking initiatives, as the 2011 Directive is transposed into national law, places governments at odds with industry and is likely to prompt an even more searching questioning of the role hotlines play and their sustainability beyond the lifetime of European funding support.

Further technological developments in combating child abuse imagery have included the use of software detection tools and upload filters by internet service providers as additional means of preventing child abuse material entering their services. As part of its effort to build a consensus among industry leaders, the European Commission with a coalition of industry CEOs has proposed the greater use of filtering technology as a proactive means of detecting and removing child abuse material at source. As with the wider use of blocking systems, such measures have raised concerns among digital rights activists concerned about the impact on fundamental freedom of expression (McNamee 2010). Yet, the strength of public and political opinion is likely to foster approaches favouring greater intervention if self-regulation is not seen as delivering adequate improvements in the area of online safety that causes most public concern.

**Conclusion**

Hotlines emerged at an early stage of the development of the internet against a background of international concern about the ease with which it could be used for illegal and harmful purposes. Against the background of high profile cases of child abuse in Belgium and in the UK, governments took notice and substantial attention was focused on the legislative, industry and regulatory responses required. Internet hotlines as a reporting and response mechanism gained strong support from the industry sector, particularly internet access providers, and were celebrated as a leading example of a self-regulating industry working with child welfare groups to deal with a phenomenon that although it did not originate with the internet, came to rapid prominence because of it (Williams 1999; Machill and Rewer 2001; Resi 2003).
Critics have argued that hotlines were only ever intended as a stop gap while governments get their own systems in order to deal with an issue of major public concern (RAND Europe 2007). Further, it is argued that the internet hotline solution has been one that has now ossified, is too reliant on European funding and is in need of review against a greatly changed technological landscape (Carr 2012). Yet, over the course of the last fifteen years, governments have more often than not prevaricated on taking more direct action while supporting industry self-regulation and awareness raising as the principal pillars for building a safer internet. The more direct interventionist approach envisaged in Directive 2011/92/EU suggests that in the battle against illegal online child abuse content, hotlines may no longer be the primary focus of policy makers’ attention.

Notes
1. CIRCAMP, the EC-funded research project (COSPOL Internet Related Child Abusive Material Project) argues that the term ‘child pornography’ is misleading and suggests that there is some form of consent involved. As the victims are children and cannot give consent, the term ‘child sexual abuse material’ is recommended as it gives a better understanding of the crime and gives more respect to the child victims. See: http://circamp.eu/index.php?option=com_content&view=article&id=10:child-pornography-versus-child-sexual-abuse-material&catid=1:project&Itemid=2
2. Recommendation 98/560/EC does not refer expressly to the problem of child pornography or child abuse material; rather “pornography” is mentioned as an example of legal content with the potential to harm minors.
3. The Daphne programme under the area of Justice is a European Union funding programme, the objective of which is to contribute to the prevention of, and the fight against all forms of violence occurring in the public or the private domain, including sexual exploitation and trafficking of human beings. See: http://ec.europa.eu/justice/grants/programmes/daphne/index_en.htm
4. SAFT – Safety, Awareness, Facts and Tools – was a pan-European project that began in 2003 which aimed to promote safe use of the Internet among children and young people. The SAFT consortium comprised seven partners in five European countries (Norway, Denmark, Iceland, Sweden and Ireland). See: http://www.saftonline.org/
5. The European Financial Coalition against Commercial Sexual Exploitation of Children Online cites an example whereby Facebook was used by a paedophile ring to exchange child abuse material. This involved a ‘group within a group’ on the Facebook platform, and coordinated by a registered sex offender in the UK. Members could only be admitted once they added further images of their own, thereby proving their credentials and gaining access to ever more serious levels of abuse. The example also illustrates the decreasing significance of a financial dimension to the criminal circulation of abuse images. In this case, images were circulated for free or in exchange for other images. European Financial Coalition (2010) 14 months on: A combined report from the European Financial Coalition 2009-2010. Brussels, European Financial Coalition against Commercial Sexual Exploitation of Children Online.
7. Note that this refers only to the filtering/blocking of illegal content as defined by so-called black lists such as those maintained by the Internet Watch Foundation or Interpol’s database. This is not to be confused with voluntary filtering schemes for legal pornography as proposed, for instance, by the UK government’s report chaired by Reg Bailey, Department

References


Staksrud, E. (Ed.) (2005) SAFT Project Final Report. Oslo, Norway: Norwegian Board of Film Classification


Chapter 3

Awareness

Strategies, Mobilisation and Effectiveness

Elisabeth Staksrud & Kjartan Ólafsson

Awareness-raising, the art of increasing people’s understanding and knowledge often with the goal of making them alter their behaviour, is a key feature in the field of internet safety. In this chapter, we briefly review the background and history of the awareness policy pillar of the European Safer Internet Programme. Then, using data from the EU Kids Online project, we raise some questions about the relative success of awareness, its relevance as a risk-reducing strategy to alter behaviour, and provide some answers to what would probably work – considering both cognitive challenges among children and youth as well as their preferences in terms of information and dissemination.

The History of Awareness Policy

The current policy discussion on children’s use of the internet includes elements of children’s perspectives, interests and rights, seeing internet access and online participation as a matter of opportunity and affordance. However, in Europe, the initial intention of the awareness action line was to make adults aware of the potential and the drawbacks of the internet, and of the means to identify useful content and block harmful content (European Commission 1999-2002). The logic of the European Commission’s awareness approach has been to move from national efforts to multiple transnational projects to(wards) a cohesive European network (DG Information Society European Commission 2001). The original objective of this action line was to “pump prime large-scale awareness actions and to provide overall coordination and exchange of experiences” (European Commission 1999-2002). Starting off by preparing the ground for awareness actions by identifying players, dissemination channels and content, the target audience was identified as parents and teachers (note, not children themselves), and the action was expected to involve industry and “multipliers” – identified as consumer associations and the education sector.
(European Commission 1999-2002). For the full-scale awareness actions, two types were envisaged: in the first phase the focus was on teachers and not on “the general public” where parents and children were seen to be part of the latter. In the second phase projects (2002-2004), the importance of identifying the state of the art was recognised, thus providing funding for awareness projects that also had an element of research and data collection. Specifically, the Safety Awareness, Facts & Tools (SAFT) project (2002-2004) was supported, providing coordinated and large-scale awareness actions aimed at teachers, children and parents, as well as other stakeholders, based on the SAFT 2003 survey of children (9-16) and parents in Denmark, Iceland, Ireland, Norway, and Sweden. The other project with a research element was MEDIAPPRO (2005-2006), focusing on the collection and analysis of existing studies of children’s use of the Internet and new technologies, providing a “complementary observation” (study), and developing a set of educational recommendations. The relevance of acquiring facts about children’s actual use of the internet and parental attitudes and fears connected with this, was demonstrated in these two projects. This, combined with Eurobarometer results on the issue made the EC decide that “knowledge enhancement” should be continued as a part of awareness policy. Consequently, three distinct awareness raising efforts were included in calls for funding: (1) to set up a “broadly-based European network”; (2) to ensure applied research on media education for all “interested” parties, such as bodies of education, NGOs, parents, teachers, industry and law enforcement (but note: not the children themselves); and (3) make use of the Eurobarometer survey to provide data about all Member States on the state of public awareness of internet safety (European Commission 2004). Then, in 2005, a new, separate action line of knowledge enhancement was introduced (see chapter 5, this volume).

Developing the idea of a European network further, and using the same model as with hotlines (see chapter 2, this volume), funding was allocated to enable national stakeholders to create awareness centres, coordinated through a pan-European network today called INSAFE. The centres’ main tasks as described by the EC are:

… raising awareness related to potential risks young people may encounter online. They develop information material; organize events such as Safer Internet Day, their biggest yearly international event; organize information sessions for parents, children and teachers. In addition, they set up youth panels to be consulted for the development of awareness raising activities, material and campaigns. (European Commission 2011)

The shift in awareness focus from parents, teachers and “multipliers” to also include children themselves raises two key questions we will address in this chapter: (1) how do awareness strategies as defined and supported by the EC
relate to the needs and preferences of the defined target groups? and (2) to what extent can children, as decision makers dealing with potentially risky and harmful online content, contacts and conduct, benefit from awareness campaigns? We frame the following discussion within “the new sociology of childhood” (James, Jenks et al. 1998), which considers children to be legitimate as well as actual decision makers, sometimes making risky choices when using the internet.

Are Awareness Strategies Relevant?

To evaluate how awareness strategies as defined and supported by the EC relate to the preferences of the defined target groups, we turn to data collected in the EU Kids Online project. The EU Kids Online survey asked parents where they would like to get information and advice about internet safety from in the future, so as to focus further awareness-raising activities, the rationale being that preference in source of information is more likely to have a positive effect in terms of actual impact of the information received.

Table 1 shows parents’ answers to two questions. First, they were asked where in general they get information and advice on safety tools and safe use of the internet from and then they were asked where they would like to get information and advice on safety tools and safe use of the internet from in the future. The most common source of information is family and friends (48%) but next in line are traditional media (32%) and then the child’s school (27%). When, on the other hand, parents are asked from where they want advice, the child’s school is the most popular choice at 43%, media in general (television, radio, newspapers or magazines) come second (32%) while friends and family occupy third place at 29%.

A direct comparison between the actual and desired sources of information suggests that more parents would like information to come to them through schools and from the government. Some 27% of parents say that they have had information or advice from schools compared to 43% who say that they would like this kind of information from schools. For government, some 7% say they have had information or advice from government compared to 20% who would prefer the government to provide them with more of this kind of information.

Table 1 also shows that when asked about their desired source of information, parents tend to cite those same sources from whom they have previously received information (see the shaded diagonal). This comparison further emphasises the importance of the school as a desired source of safety advice for parents. For most of the different sources of information around half of those who have had information on safety tools and safe use of the internet from that particular source mention that same source when asked where they would like
to get advice from in the future. For the school, however, this figure is three out of four. Finally, Table 1 shows a clear appetite for more information on internet safety amongst parents as only around 9% say that they do not want further information on internet safety.

Turning to children and their information needs, the family is the most common source of safety information for children (as for parents) with 63% of children saying that their parents have suggested ways for them to use the internet safely. Some 58% say that they have received safety advice from teachers, 44% from peers and 47% say that they have received such advice from other relatives.

Table 2 shows the percentage of children who say that one of their parents has suggested ways for them to use the internet safely compared with different ways in which parents themselves have received information on safe use of the internet. The idea here is to see if parents who have received advice from different sources are more or less likely to have given advice to their child
(as reported by the children). As it turns out there is little (surprisingly little perhaps) difference between different sources of information when it comes to how likely it is that children receive online safety information from their parents. It is only parents who have had no such advice or who get it from their child who are less likely to be reported by their child to have given advice.

Table 2. Children Who Say that Their Parent (or either of their parents) Has Suggested Ways for Them to Use the Internet Safely

<table>
<thead>
<tr>
<th>% children who say that their parents (or either of their parents) has suggested ways for them to use the internet safely</th>
<th>9-10 yrs</th>
<th>10-12 yrs</th>
<th>13-14 yrs</th>
<th>15-16 yrs</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td>School</td>
<td>73</td>
<td>71</td>
<td>75</td>
<td>63</td>
<td>71</td>
</tr>
<tr>
<td>TV etc</td>
<td>73</td>
<td>72</td>
<td>68</td>
<td>65</td>
<td>69</td>
</tr>
<tr>
<td>ISP's</td>
<td>78</td>
<td>79</td>
<td>73</td>
<td>65</td>
<td>74</td>
</tr>
<tr>
<td>Government</td>
<td>75</td>
<td>74</td>
<td>76</td>
<td>62</td>
<td>72</td>
</tr>
<tr>
<td>NGO's</td>
<td>71</td>
<td>78</td>
<td>70</td>
<td>64</td>
<td>71</td>
</tr>
<tr>
<td>Websites</td>
<td>77</td>
<td>79</td>
<td>76</td>
<td>65</td>
<td>74</td>
</tr>
<tr>
<td>Manufacturers</td>
<td>75</td>
<td>76</td>
<td>74</td>
<td>66</td>
<td>73</td>
</tr>
<tr>
<td>Family and friends</td>
<td>72</td>
<td>72</td>
<td>71</td>
<td>61</td>
<td>69</td>
</tr>
<tr>
<td>From child</td>
<td>65</td>
<td>66</td>
<td>65</td>
<td>55</td>
<td>62</td>
</tr>
<tr>
<td>Other sources</td>
<td>74</td>
<td>76</td>
<td>74</td>
<td>70</td>
<td>73</td>
</tr>
<tr>
<td>No information</td>
<td>48</td>
<td>47</td>
<td>36</td>
<td>33</td>
<td>40</td>
</tr>
</tbody>
</table>

So, are awareness strategies relevant? Based on the findings from EU Kids Online as presented above, the answer is yes: most parents receive some kind of information on safe use of the internet, and most parents want to receive such information in the future. The 37% of parents who have not received any information in the past and would not like to do so in the future (Table 1) suggests that some parents either are not concerned or do not see the need for them to concern themselves with their children’s safety on the internet. The results suggest that even if parental awareness is an important element of safe use, it is not on its own sufficient. Table 2 shows that there is no ‘one size fits all’ solution. Most parents will disseminate information about safe use to their children, regardless of the method by which they acquired it but those parents who have not themselves received information on safe use of the internet are also less likely than parents who have received advice to have given such advice to their children.

Can Children Benefit from Awareness Campaigns?

Our assumptions concerning the concept of media risk are based on the perception that the future and its outcome is seen as influenced, at least in part,
by human beings. Hence, it should be possible, with the right approach, to prevent potential hazards or to mitigate their consequences (Ewald 1993 cited in Renn and Klinke 2001). Assessing effective risk management strategies, central to the discourse of online risk, is dependent on understanding how individuals decide to – or not to – engage in risky behaviour. Awareness campaigns directed towards children will typically aim at informing them about what is considered “good” or “safe” behaviour, and discourage behaviour that is “risky” or “harmful” or simply “not wanted”. Within the framework of the European Safer Internet Programme (SIP), the knowledge enhancement action line has increasingly informed awareness efforts, typically by the use of evidence in the form of quantitative data and statistics. The central categories for risk assessment are the extent of damage (negatively evaluated consequences of human activities) and the probability of occurrence (Renn and Klinke 2001). While uncertainty is a fundamental characteristic of risk, one can use indicators to determine the probability of occurrence and the extent of damage. While one cannot always assess the certainty of single incidents, the probability of such incidents can often be determined, as demonstrated in various analyses of EU Kids Online data. From these findings emerges the understanding that most – if not all – children will at some point experience online risk and engage in risky behaviour (Livingstone, Haddon et al. 2011).

Thus, in terms of safety it becomes important to try to also create awareness that might make children, and often specific demographic groups of children, alter their behaviour in favour of safer conduct. But, to what extent can children benefit from awareness campaigns in the sense that they might alter their behaviour in order to avoid risky online situations? If awareness raising strategies are to be effective, they need to be informed by not only children’s actual behaviour, thoughts and feelings when engaging online, but also by their decision making processes. In the following, we elaborate on how decisions concerning risks are made on the individual and group level, by reviewing findings from cognitive psychology and neurobiology. Then, the issue of children vs. adults will be addressed: do children make risky decisions the same way as adults do, and if not, what are the prescriptive – and practical – implications for online awareness campaigns?

**Children as Decision Makers**

Simplified, one can say that traditional research in the field of children and decision making/risk has evolved from “thin” theories of rationality (see Elster 1983). From traditions such as thin theory and cognitive psychology, and the popular belief that, when it comes to decision making, children are a homogenous risk-taking group, come the often referred to claims (Reyna and Farley 2006; Stanovich 2006) that:
1. Children (adolescents) have strong feelings of *invulnerability* and
2. Children (adolescents) *underestimate* the probabilities of negative outcomes

But, this area of research, often from the fields of psychology and biology (brain-research), is scattered with counterintuitive findings. For instance: a study of young smokers showed how participants, knowing the general harm caused by smoking, perceived themselves to be at little or no risk as they planned to stop smoking before any health damage could occur (Slovic 2000). Why so? While the chances of a specific risk becoming reality can often be assessed by scientific methods using various indicators as described above, the *perception of risk* is more personal, based on one’s own experiences, level of information, and intuitive heuristics that have been developed through biology and cultural evolution (Renn and Klinke 2001). The technical and natural science-based risk concepts ignore these dimensions, but within psychological and social scientific notions of risk – such as the ones we are dealing with here – understanding risk *perception* is key to understanding risk and related decision making. The perception of risk can therefore be seen as a potential outcome of information gathering by a complex set of methods, including subjective connotations and emotions.

Further insight can be offered from the field of cognitive psychology where studies show that people use heuristics or rules of thumb rather than probability assessment (Kahneman and Tversky 1979; Jackson, Allum et al. 2005). Also, experiments have shown how individuals *anchor*, meaning that they will overly rely on specific pieces of information or specific values, something that will usually create a bias towards that value when engaging in normal decision making processes (Tversky and Kahneman 1974; Kahneman and Tversky 1979; Lovallo and Kahneman 2003). This form of *focusing effect*, where the decision maker presents a cognitive bias placing too much importance on one aspect of a situation, causes errors in terms of accurately predicting future outcomes. These types of assessments also lead to inconsistent preferences when the same choice is presented in different forms (Kahneman and Tversky 1979). In summary, findings from cognitive psychology suggest (Jackson, Allum et al. 2005) that in relation to *representativeness*, people tend to evaluate the chances of X as originating from Y to the extent that X resembles Y (representativeness heuristic). In relation to *availability*, the size of a class tends to be judged by the ease with which instances of it can be retrieved by memory (e.g. if an online risk has been prominently placed in the news, such as the issue of pornography), its probability of occurrence will be judged as higher than risks that cannot be as easily conceptualized or remembered (such as children being deviant online). In addition, research on prospect theory (Kahneman and Tversky 1979) shows how individuals *over-weight low-probability events*,

63
and underestimate high-probability events (e.g. parents consider the threat of a paedophile grooming their child online greater than the probability of their child bullying others online).

To illustrate, to assess parents’ worries about children’s online experiences, the EU Kids Online survey asked parents about whether or not they worried about nine different things, including their children being contacted by strangers on the internet and seeing inappropriate material on the internet. The question was phrased as follows: ‘Thinking about your child, which of these things, if any, do you worry about a lot?’ Around half of parents said it was how the child is doing at school. 43 per cent worry a lot that the child gets injured on the roads. The two internet-related items on the list (being contacted by strangers and seeing inappropriate material on the internet) is mentioned by a third of parents.

Table 3. Parents’ Answers to Which Things They Worry About a Lot, by Age and Gender

<table>
<thead>
<tr>
<th></th>
<th>9-12 years</th>
<th></th>
<th>13-16 years</th>
<th></th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Boys</td>
<td>Girls</td>
<td>Boys</td>
<td>Girls</td>
<td>All</td>
</tr>
<tr>
<td>How they are doing at school</td>
<td>53</td>
<td>51</td>
<td>54</td>
<td>48</td>
<td>51</td>
</tr>
<tr>
<td>Being injured on the roads</td>
<td>45</td>
<td>45</td>
<td>42</td>
<td>40</td>
<td>43</td>
</tr>
<tr>
<td>Being treated in a hurtful or nasty way by other children</td>
<td>40</td>
<td>43</td>
<td>29</td>
<td>31</td>
<td>35</td>
</tr>
<tr>
<td>Being a victim of crime</td>
<td>34</td>
<td>35</td>
<td>35</td>
<td>36</td>
<td>35</td>
</tr>
<tr>
<td>Being contacted by strangers on the internet</td>
<td>32</td>
<td>36</td>
<td>29</td>
<td>36</td>
<td>33</td>
</tr>
<tr>
<td>Seeing inappropriate material on the internet</td>
<td>34</td>
<td>35</td>
<td>30</td>
<td>30</td>
<td>32</td>
</tr>
<tr>
<td>Drinking too much alcohol/taking drugs</td>
<td>21</td>
<td>19</td>
<td>31</td>
<td>28</td>
<td>25</td>
</tr>
<tr>
<td>Getting into trouble with the police</td>
<td>20</td>
<td>18</td>
<td>25</td>
<td>19</td>
<td>20</td>
</tr>
<tr>
<td>Their sexual activities</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>20</td>
<td>16</td>
</tr>
<tr>
<td>None of these</td>
<td>20</td>
<td>21</td>
<td>20</td>
<td>22</td>
<td>21</td>
</tr>
</tbody>
</table>

Interestingly, roughly the same percentage mentions ‘being contacted by a stranger’ as ‘seeing inappropriate material’ though at the same time very few children have been bothered after meeting online contacts offline. Also, some 3 per cent of the parents interviewed in the EU Kids Online survey said they believed their child had bullied another child online. In comparison, some 33 per cent of the parents say that they worry a lot about their child being contacted by strangers on the internet.

What does this mean in practice? The perception of risk often seems to override the research and available facts, hence turning the management of risk into something with embedded irrationality. For instance: when parents were asked how likely they think it is that their child will experience problems on the internet in the next six months some 5 per cent say that they think it is very likely. A further 23 per cent say they think it is fairly likely, some 45 per cent that it is not very likely and some 28 per cent that it is not likely at all (Living-
At the same time, some 12 per cent of the children said that they had been bothered by something online (Livingstone, Haddon, Görzig and Ólafsson 2011: 46). It can be debated whether this means that parents as a group correctly estimate the risks associated with children’s internet use. However, some parents clearly overestimate the risks and some underestimate them. Thus, when prioritizing policy and awareness efforts in a situation with limited resources available, one must decide: should one prioritize based on fears or facts? While both can potentially be a problem, the appropriate prescriptive measures might not be the same.

**Children’s Decision Making About Risk**

While public perceptions of risk are subject to systematic errors and biases when compared to probability calculations, this does not mean that these perceptions are not valid. This also means that the social meaning of any given risk cannot be controlled by any single individual (see, for instance, Lessig 1995), or a single organization. For children/adolescents/teens/young adults, the social meaning of specific risks and risk-taking often differs from that of their parents and teachers. To point to a typical Nordic example: there are times in a child’s life when wearing proper winter clothing (not to mention winter hats) is at odds with what is considered cool, and perceived as rather pathetic within the peer group, making it a common occurrence during the cold Winter mornings to see shivering children taking off their coats/hats/muffs/mittens when out of parental sight, stashing them until it is time to return home. The risk of being uncool trumps physiological fact and comfort.

So – what do we know about children as decision makers about risk? The path chosen for the following discussion leans heavily on the extensive scientific review of risk and rationality in adolescent decision making by Reyna and Farley (2006). Providing a “metatheoretical reorientation” (Stanovich 2006), they point to studies concluding that adolescents are capable of rational decision making to achieve their goals, but much will depend on the particular situation where the decision making is taking place. The extensive research review (note: primarily based on risk studies relating to health-issues, many done in laboratory (controlled) settings) shows how (perhaps counter-intuitively):

- Children (adolescents) do not perceive themselves as being invulnerable
- Children (adolescents) typically overestimate important risks (e.g. HIV, lung cancer)
- Children (adolescents) tend to underestimate harmful consequences and long term effects (such as addiction)
- Children (adolescents) exhibit an optimist bias, viewing their own risk occurrences as less than those of comparable peers$^6$
• Children (adolescents) belonging to an objectively higher risk group will sometimes rate their risk as higher and sometimes as lower than lower-risk groups rate themselves.

Thus, compared to findings on adults, children consider themselves to be more vulnerable (point 1), and feel more exposed to important risks than adults (point 2) having no higher prevalence of an optimist bias than for adults (point 4), but may not consider the consequences to be relevant (point 3). They may sometimes rate themselves as having lower or higher risk, depending on the particular risk assessment situation (point 5). Factors influencing decision making include the presence of peers, “spur of the moment”/“in the heat of passion”, unfamiliar situations, whether one is dealing with potential short-term vs. long term consequences, and when behavioural inhibition is required for good outcomes (Reyna and Farley 2006). In these situations, adolescents are prone to reason more poorly than adults.7

Linking these findings to our field of internet risk and safety, Table 4 presents an ordered logistic regression which was conducted to measure to what extent ‘actual’ digital skills (as measured by eight questions8) relate to ‘perceived’ skills as measured by the response of the question ‘I know lots of things about using the internet’. The question on perceived skills had three categories, ‘not true’, ‘a bit true’ and then ‘very true’. The model shows how the probability of selecting a higher category (i.e. having higher perceived skills) changes for the independent variables.

<table>
<thead>
<tr>
<th>Table 4. Ordered Logistic Regression Model of how Children Answer the Question ‘I Know Lots of Things about Using the Internet’ (not true as a reference category)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Constant  -2.12  0.060  -35.50  0.00  0.12</td>
</tr>
<tr>
<td>Gender (girls)  0.08  0.058  1.16  0.25  1.08</td>
</tr>
<tr>
<td>Age  0.15  0.011  14.14  0.00  1.16</td>
</tr>
<tr>
<td>Digital safety and literacy skills  0.14  0.010  13.69  0.00  1.15</td>
</tr>
<tr>
<td>Time spent online  0.23  0.016  13.23  0.00  1.26</td>
</tr>
<tr>
<td>Number of online activities  0.15  0.006  24.95  0.00  1.16</td>
</tr>
<tr>
<td>Gender X skills  -0.01  0.014  -0.16  0.87  0.99</td>
</tr>
<tr>
<td>-2 Log likelihood  -10680</td>
</tr>
<tr>
<td>Chi-square  3787.00</td>
</tr>
<tr>
<td>P  0.00</td>
</tr>
<tr>
<td>Pseudo R²  0.15</td>
</tr>
</tbody>
</table>

The results show (as would be expected) that children with more actual skills tend to rate themselves higher when asked if it is true that they know lots about using the internet. Indeed for each point a child scores higher on the 8 point scale for digital literacy and safety skills, their probability of selecting a higher
category on the perceived skills scale goes up by 15 per cent. However, age has approximately the same effect and so even when actual skills, number of online activities and time spent online have been taken into account, there is still a correlation between age and perceived skills. In other words, even for children who have the same number of actual skills their probability of selecting both the ‘Not true’ and the ‘A bit true’ options decrease and their likelihood of selecting ‘Very true’ goes up.

Figure 1 shows how perceived skills are related to actual skills. Here it is possible to see visually the strong link between actual skills and perceived skills but still children who score zero on the digital skills index have somewhere around 15 per cent probability of selecting the option that it is very true that they know lots about using the internet. In other words, a sizeable group of children clearly overestimates their own abilities in using the internet.

Figure 1. Predicted Probability for the Three Answer Categories of ‘I Know Lots of Things About Using the Internet’ by Gender and Skills for Children aged 14 years

The tendency to overestimate one’s own abilities on the internet is further linked to age, with older children being more reluctant to say that it is not true that they know lots about using the internet even if they measure low on the actual skills. Thus, a 16 year old child who has a score of zero on the measurement for actual skills still only has a probability of around 25 per cent of selecting the answer category ‘not true’ when asked if they know a lot about using the internet.
Does Awareness-raising Work?

It is of course impossible to draw conclusions about causal effects using cross-sectional data like the EU Kids Online survey. It is however possible to look at the extent to which the different ways in which children say that they have had information on safe use of the internet is related to their probability of having encountered certain online risks.

A logistic regression was conducted to examine whether the probability (in odds ratios) of encountering each of the five different risks differs between those who have received advice on safe use of the internet in different ways (Table 5) and controlling for gender, age, time spent online and frequency of using the internet.

**Table 5.** Logistic Regression Models of the Log Odds of a Child Encountering Risks on the Internet, by Where They Have Received Advice on Safe Use of the Internet

<table>
<thead>
<tr>
<th></th>
<th>Seeing sexual images on any websites</th>
<th>Being bullied on the internet</th>
<th>Meeting new people</th>
<th>Receiving sexual messages</th>
<th>Negative user generated content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Constant</td>
<td>0.10</td>
<td>0.02</td>
<td>0.03</td>
<td>0.06</td>
<td>0.10</td>
</tr>
<tr>
<td>Gender (girls)</td>
<td>0.66</td>
<td>1.65</td>
<td>1.12</td>
<td>0.84</td>
<td>1.41</td>
</tr>
<tr>
<td>Age</td>
<td>1.28</td>
<td>1.03</td>
<td>1.30</td>
<td>1.32</td>
<td>1.24</td>
</tr>
<tr>
<td>Time spent online (hours)</td>
<td>1.24</td>
<td>1.40</td>
<td>1.43</td>
<td>1.28</td>
<td>1.30</td>
</tr>
<tr>
<td>Use the internet daily</td>
<td>2.11</td>
<td>1.61</td>
<td>2.04</td>
<td>1.61</td>
<td>1.39</td>
</tr>
<tr>
<td>Advice on internet safety from...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Friends</td>
<td>0.78</td>
<td>n.s.</td>
<td>n.s.</td>
<td>n.s.</td>
<td>n.s.</td>
</tr>
<tr>
<td>Teachers</td>
<td>n.s.</td>
<td>n.s.</td>
<td>n.s.</td>
<td>n.s.</td>
<td>n.s.</td>
</tr>
<tr>
<td>Parents</td>
<td>n.s.</td>
<td>n.s.</td>
<td>0.73</td>
<td>0.83</td>
<td>0.86</td>
</tr>
<tr>
<td>Youth or church or social worker</td>
<td>1.17</td>
<td>n.s.</td>
<td>n.s.</td>
<td>n.s.</td>
<td>1.18</td>
</tr>
<tr>
<td>Librarian</td>
<td>1.33</td>
<td>1.38</td>
<td>n.s.</td>
<td>1.33</td>
<td>1.49</td>
</tr>
<tr>
<td>Other relative</td>
<td>n.s.</td>
<td>1.14</td>
<td>n.s.</td>
<td>n.s.</td>
<td>1.13</td>
</tr>
<tr>
<td>Someone whose job is to give advice over the internet</td>
<td>1.26</td>
<td>1.26</td>
<td>1.31</td>
<td>1.20</td>
<td>n.s.</td>
</tr>
<tr>
<td>Websites</td>
<td>1.54</td>
<td>1.21</td>
<td>1.31</td>
<td>1.39</td>
<td>1.46</td>
</tr>
<tr>
<td>Television, radio, newspapers or magazines</td>
<td>1.19</td>
<td>n.s.</td>
<td>1.26</td>
<td>1.21</td>
<td>1.31</td>
</tr>
<tr>
<td>Internet service provider</td>
<td>1.24</td>
<td>n.s.</td>
<td>n.s.</td>
<td>1.20</td>
<td>1.34</td>
</tr>
<tr>
<td>-2 Log likelihood</td>
<td>15107</td>
<td>8398</td>
<td>10412</td>
<td>10712</td>
<td>15850</td>
</tr>
<tr>
<td>Cox &amp; Snell R²</td>
<td>0.11</td>
<td>0.02</td>
<td>0.08</td>
<td>0.07</td>
<td>0.09</td>
</tr>
<tr>
<td>Nagelkerke R²</td>
<td>0.19</td>
<td>0.06</td>
<td>0.17</td>
<td>0.12</td>
<td>0.13</td>
</tr>
<tr>
<td>Chi-square (model)</td>
<td>2225</td>
<td>454</td>
<td>1532</td>
<td>959</td>
<td>1371</td>
</tr>
<tr>
<td>df (model)</td>
<td>14</td>
<td>14</td>
<td>14</td>
<td>14</td>
<td>14</td>
</tr>
</tbody>
</table>

Gender, age, amount of internet use and frequency of use are included in the model as control variables which have been shown in general to be related...
to the likelihood of encountering risk (see for example Livingstone, Haddon, Görzig & Ólafsson 2011). For the different ways in which children have received information on safe use of the internet, the general pattern seems to be that only advice from friends and parents is linked to a decrease in the likelihood of encountering risks. All other ways of receiving advice are, if anything, related to a higher likelihood of encountering risks. As pointed out before, it is impossible to draw any conclusions about cause and effect here. However, it is possible to hypothesize that advice is sought as a reaction to unpleasant experiences, also that advice increases the likelihood of risks by encouraging the children to explore new things and finally that the correlation observed between advice and risks is merely due to other unobserved variables.

The effect of advice from friends seems to be limited purely to the likelihood of seeing sexual images. If a child says that his or her friends have suggested ways to use the internet safely then the likelihood of them having seen sexual images on any websites is decreased by about 22 per cent. Why this effect is observed only for this particular risk is difficult to say but it might in some way be due to the context in which these children use the internet.

Receiving safety advice from parents is associated with a decrease in the likelihood of meeting online contacts offline, receiving sexual messages and encountering negative user generated content. Thus advice from parents is the factor that can be most consistently related to a lower risk of encountering risks and the reduction is somewhere between 14 to 27 per cent. No effect is found for teachers however. Most other sources of advice on internet safety are then associated with either no difference or an increase in the likelihood of encountering risks.

What then about efforts to alter the behaviour of those not encountering risk, but actually causing risk for others through negative behaviour? The same logistic regression was conducted to examine whether the probability (in odds ratios) of acting in a nasty or hurtful way towards others on the Internet or sending or posting sexual messages of any kind differs between those who have received advice on safe use of the internet in different ways (Table 6) and controlling for gender, age, time spent online and frequency of using the internet.

For the different ways in which children have received information on safe use of the internet, the general pattern seems to be that only advice from parents is linked to a decrease in the likelihood of acting in a nasty or hurtful way towards others. All other ways of receiving advice are, if anything, related to a higher likelihood of acting in a nasty or hurtful way towards others and of sending or posting sexual messages online.
Table 6. Logistic Regression Models of the Log Odds of a Child Acting in a Negative Way Towards Others on the Internet, by where They Have Received Advice on Safe Use of the Internet

<table>
<thead>
<tr>
<th></th>
<th>Bullying others</th>
<th>Sending sexual messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Constant</td>
<td>0.01</td>
<td>0.01</td>
</tr>
<tr>
<td>Gender (girls)</td>
<td>n.s.</td>
<td>0.62</td>
</tr>
<tr>
<td>Age</td>
<td>1.15</td>
<td>1.27</td>
</tr>
<tr>
<td>Time spent online (hours)</td>
<td>1.54</td>
<td>1.33</td>
</tr>
<tr>
<td>Use the internet daily</td>
<td>2.18</td>
<td>n.s.</td>
</tr>
<tr>
<td>Advice on internet safety from...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Friends</td>
<td>n.s.</td>
<td>n.s.</td>
</tr>
<tr>
<td>Teachers</td>
<td>n.s.</td>
<td>1.25</td>
</tr>
<tr>
<td>Parents</td>
<td>0.83</td>
<td>n.s.</td>
</tr>
<tr>
<td>Youth or church or social worker</td>
<td>1.52</td>
<td>1.44</td>
</tr>
<tr>
<td>Librarian</td>
<td>n.s.</td>
<td>n.s.</td>
</tr>
<tr>
<td>Other relative</td>
<td>n.s.</td>
<td>n.s.</td>
</tr>
<tr>
<td>Someone whose job is to give advice over the internet</td>
<td>1.28</td>
<td>n.s.</td>
</tr>
<tr>
<td>Websites</td>
<td>1.30</td>
<td>n.s.</td>
</tr>
<tr>
<td>Television, radio, newspapers or magazines</td>
<td>n.s.</td>
<td>n.s.</td>
</tr>
<tr>
<td>Internet service provider</td>
<td>n.s.</td>
<td>n.s.</td>
</tr>
<tr>
<td>-2 Log likelihood</td>
<td>4336</td>
<td>3628</td>
</tr>
<tr>
<td>Cox &amp; Snell R²</td>
<td>0.02</td>
<td>0.02</td>
</tr>
<tr>
<td>Nagelkerke R²</td>
<td>0.10</td>
<td>0.06</td>
</tr>
<tr>
<td>Chi-square (model)</td>
<td>435</td>
<td>217</td>
</tr>
<tr>
<td>df (model)</td>
<td>14</td>
<td>14</td>
</tr>
</tbody>
</table>

The Cognitive Challenges of Awareness Strategies for Children

Understanding how children and adolescents approach unhealthy risky situations and how they make decisions about their own behaviour relating to perceived risk, is key to developing efficient risk management strategies, reducing the probability of occurrence and the extent of damage. Such an understanding should therefore be directly relevant when considering societal regulatory schemes such as controlling access and content – technically, physically, legally and/or by self-regulatory means – and the institutionalization of preventive measures such as national awareness campaigns and educational programmes as this goes to the core of their legitimacy.

In Europe, publicly driven risk management tends towards a more individualized institutionalization (Beck and Beck-Gernsheim 2001; Beck 2007) where the individual is ultimately required to assume responsibility
for decision making – in effect decisions on risk management, instead of pre-determined state regulation – based on the premise that there will be a choice or several choices, and that the decision made should be rational. In order to make rational decisions on a complex area, the decision has to be informed. This has led to a preponderance of educational programmes aimed at children, parents, teachers and others, not only in the field of internet safety, but also in other risk management fields pertaining to children and adolescents, such as safe sex, safe driving, smoking, binge drinking, etc. However, according to (some) neurobiologists, educational programmes are destined to have little effect in reducing adolescent risk-taking (Steinberg 2008), because:

The problem is not what adolescents know, but what they do. Indeed, adolescents often know plenty. They have relevant information about relevant risks. They act recklessly not because they are ill-informed, but because their dopaminergic system is developing more rapidly than their cognitive control system. (Sunstein 2008)

Reviewing more recent literature on neurobiology findings, Staksrud (2011) found direct implications for consideration in relation to awareness campaigns (Table 7).

One concrete implication for policy is that considering only this path, younger children and adolescents should be sheltered from risky experiences and supervised to thwart negative exploration as they will not be able to benefit from negative experiences. Quite the contrary: risk taking that does not result in negative experiences might increase feelings of invulnerability (Reyna and Farley 2006). However, considering other aspects, such as how we view children, how we consider the internet as a vital tool for education, entertainment and development (as described in chapter 10, this volume), this creates an obvious tension between the consequences of risky decisions, and how to protect children from such consequences, the regulatory regimes within EU Member States, and the rights of children as people and as citizens in democratic states to information and participation.

These findings also pose (yet another) methodological problem when researching children and risk and making descriptive assessments and predictive recommendations based on the self-assessment of children in questionnaires about their future risk practices. The optimist bias of how well one’s future self will behave (note: existing, but not higher than for adults) may result in a highly inaccurate starting point for research, child protection and policy making.
### Table 7. Prescriptive Implications from Research

<table>
<thead>
<tr>
<th>Description</th>
<th>Prescriptive Implications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Descriptive (Findings)</strong></td>
<td><strong>Potentially effective</strong></td>
</tr>
<tr>
<td>Risk taking increase between childhood and adolescents and decrease between adolescents and adulthood (see Steinberg, 2008)</td>
<td>General rules and regulations</td>
</tr>
<tr>
<td>Adolescents feel vulnerable and overestimate risk (see Reyna &amp; Farley, 2006)</td>
<td>Cue negative gist (see Rivers, Reyna, &amp; Mills, 2008)</td>
</tr>
<tr>
<td>Adolescents learn little from negative outcomes</td>
<td>Experience</td>
</tr>
<tr>
<td>Adolescents use conscious liberation</td>
<td>Supervision and monitoring</td>
</tr>
<tr>
<td>Benefits loom over risks</td>
<td>Focus on potential long-term consequences</td>
</tr>
<tr>
<td>Self-control over temptations are dependent on the ability to identify conflicts (see Fishbach &amp; Converse, 2011)</td>
<td>Focus on single incidents</td>
</tr>
<tr>
<td>Risk taking is more likely to take place in groups</td>
<td>Use peer “meaning entrepreneurs” to create new social meanings in groups</td>
</tr>
<tr>
<td>Image based systems works outside explicit awareness: media presentations, behaviour of friends and parental behaviour can affect the valence associated with various prototypes (see Sunstein, 2008, p. 149)</td>
<td>Heuristic approach working directly on mental images (see Gerrard, Gibbons, Houlihan, Stock, &amp; Pomery, 2008) alter the social meaning of reckless behaviour, e.g., cool/positive images associated with healthy choices, and bad/negative images associated with unhealthy choices. Making cues personal and emotional.</td>
</tr>
<tr>
<td>Adolescents lack neural hardware to generate behavioural alternatives in situations demanding a response (see Baird &amp; Fugelsang, 2004, p. 1801)</td>
<td>General recommendations like “just say no”</td>
</tr>
<tr>
<td><strong>Note:</strong> Adapted from Staksrud 2011: 124.</td>
<td></td>
</tr>
</tbody>
</table>

### Conclusions

The results and analyses provided in this chapter show that both the individual and public perceptions of risks and the likelihood of risk occurrence are influenced by emotions, experiences, connotations, in addition to mere probability calculations. Furthermore, findings from biology, in particular neurobiology, suggest that children make decisions involving risk differently to adults.
In addition, given the differences between children and adults regarding how one approaches issues of risk, differences in their *behaviour willingness*, it is also likely that the perception of what online risk is, and especially how severe the potential consequences of a particular risk might be, will differ between children and adults – and consequently also between policy makers and awareness raisers on one side and the historically new primary target group (children) on the other. It is also likely that the ranking of risks – assessing the probability of occurrence vs. the potential extent of damage – will differ, as external and internal factors influence individuals’ perception of online risk. In other words, fears might be dispersed, covering a large set of online activities and experiences.

In conclusion, and in line with the view argued by Renn and Klinke (2001), when considering the issue of risks associated with media use in general and internet use in particular, we need to include both the methods of technical and natural scientific assessment, and risk perception, seeing the latter as an integral part of (rational) risk evaluation. Or, to put it another way, risk perception is not based on rational thinking and damage-probability confidence interval calculations. And, studies have revealed how people will orient their behaviour according to their perceptions. Perceived risks can generate symptoms in the same way that the real potential of risk can (Renn and Klinke 2001). Thus, awareness campaigns must, if they are to be successful, take on board the understanding not only of the subjective nature of risk perception, but also the complex field of how children make risky decisions.

Notes
3. A random stratified sample of approximately 1000 internet-using children aged 9-16 years was interviewed in each of 25 European countries (Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Lithuania, the Netherlands, Norway, Poland, Portugal, Romania, Slovenia, Spain, Sweden, Turkey and the UK). The countries were selected to represent the economic, geographic and cultural diversity of European countries. The total sample size for children was 25,142; additionally, one parent (the one who knew most about their internet use) of each child was interviewed. The questionnaire was carefully designed to be used in 24 languages and tested using both

Acknowledgements
The authors acknowledge the support of the VITOVIN project (CZ.1.07/2.3.00/20.0184), which is co-financed by the European Social Fund and the state budget of Czech Republic.
cognitive testing and pilot testing to aid completion by children. Interviews took place during spring and summer 2010 in children’s homes, conducted face-to-face but with private questionnaire completion (computer-assisted or pen-and-paper) for sensitive questions related to risk. Average interview time per child was 45 minutes London School of Economics and Political Science and IPSOS (2011), EU Kids Online II, user guide and technical report. London, LSE.

4. The most common risk of children’s internet use in Europe is associated with communicating online with someone the child has not met face-to-face before – characteristic of 30% of 9-16 year olds (see Livingstone, Haddon Görzig and Ólafsson, 2011: 82). It will be noted that such communication is, also, an opportunity, for whether the child is thereby making a new friend or being contacted by a stranger is not easy to determine in a survey. Thus this finding should be treated with caution. Almost as common is exposure to one or more of the types of potentially harmful user-generated content asked about (concerned with hate, pro-anorexia, self-harm, drug-taking or suicide) – this was experienced by 21% of 11-16 year olds (see Livingstone, Haddon Görzig and Ólafsson, 2011: 98). Rather less common is children’s exposure to sexual images online (14% of 9-16 year olds – see Livingstone, Haddon Görzig and Ólafsson, 2011: 50) or to sexual messages (15% of 11-16 year olds – see Livingstone, Haddon Görzig and Ólafsson, 2011:74). Less common still is the misuse of personal data (misuse of the child’s password, information or money) – 9% of 11-16 year olds (see Livingstone, Haddon Görzig and Ólafsson, 2011: 100). This is followed by going to meetings offline with people first met online (9% of 9-16 year olds – see Livingstone, Haddon Görzig and Ólafsson, 2011: 85). Last, and least common is ‘cyberbullying’ – being sent nasty or hurtful messages online is reported by 6% of 9-16 year olds – see Livingstone, Haddon Görzig and Ólafsson, 2011, p. 62). All risks are increased by age (Livingstone, Haddon Görzig and Ólafsson, 201: 134). Looking across all the risks asked about in the EU Kids Online survey, 14% of 9-10 year olds have encountered one or more of these. This percentage rises sharply to 33% of 11-12 year olds and rises again to 49% for the 13-14 year olds. Among the 15-16 year olds 63% report encountering one or more of the risks asked about in the survey, the average across all 9-16 year olds being 41%.

5. This part has also been published in part in Staksrud (2013)

6. This can also be found among adults, see for instance Quadrel, Fischhoff & Davis Quadrel, M., B. Fischhoff, et al. (1993) ‘Adolescent (in)vulnerability’, Am Psychol., 48(2): 102-16. for a study where both adults and children are included and compared.

7. In general the review on cognitive and neurobiological findings refer to adolescents, not all children. It should however be emphasized that framing effects in decision making (= shift in choices for the same options when they are described in terms of gains rather than losses) increase during childhood and adolescence. Preschoolers have been shown to make choices based on the quantitative bottom line involving both the probability and outcome decisions, children in elementary school have been shown to make choices based on what gives more benefits, ignoring dimensions of probability and their potential magnitude, adolescents are more likely to be qualitative reasoners, preferring the sure-but-smaller-options seeking to have some gain rather than all lost, while adults have been shown to prefer making such decisions qualitatively rather than quantitatively. See Reyna & Farley (2006: 31).

8. Which of these things do you know how to do on the internet? Please say yes or no to each of the following: Bookmark a website. Block messages from someone you don’t want to hear from. Find information on how to use the internet safely. Change privacy settings on a social networking profile. Compare different websites to decide if information is true. Delete the record of which sites you have visited. Block unwanted adverts or junk mail/spam. Change filter preferences

References


Chapter 4

Regulation and Legislation

Sharon McLaughlin

Regulation is a phenomenon that is notoriously difficult to define with clarity and precision, as its meaning and the scope of its inquiry are unsettled and contested. […] At their narrowest, definitions of regulation tend to centre on deliberate attempts by the state to influence socially valuable behaviour which may have adverse side-effects by establishing, monitoring and enforcing legal rules. At its broadest, regulation is seen as encompassing all forms of social control, whether intentional or not, and whether imposed by the state or other social institutions. (Morgan and Yeung 2007: 3-4)

While the concept of regulation is difficult to delineate in any concrete manner, it is generally understood – at least from a European perspective – to apply to various means of achieving public policy objectives. According to a report published in 2006 by the European Commission Directorate for Information Society and Media, “[r]egulation within a given society can be described as being positioned in the triangle of state, economy and civil society” (Hans-Bredow Institut 2006). The report makes it clear that there is no uniform European conception of regulation; rather the meaning ascribed to the concept changes commensurate with changes in democracy, politics and policy. Conceptually speaking, regulation may be divided into three distinct stages: (1) the legislative stage, which involves the creation of appropriate rules; (2) the enforcement stage, which refers to the methods adopted to ensure effective implementation of these rules; and (3) the adjudication stage, which refers to the processes through which violations of the rules are assessed and appropriate sanctions imposed (Campbell 1998-1999). Regulation may take many forms, including command-and-control regulation, self-regulation and co-regulation – each of which will be considered in this chapter. Regulation of the audiovisual media sector is considered particularly problematic in light of the fact that considerable importance is attached to the functions performed by the mass media (Hans-Bredow Institut 2006). For example, Article 17 of the United Nations
Convention on the Rights of the Child, which deals with the right of access to information and the role of the mass media, expressly recognises “the important function performed by the mass media” (United Nations 1989). In addition, the EU Agenda for the Rights of the Child explicitly acknowledges that “[o]nline technologies bring unique opportunities to children and young people by providing access to knowledge and allowing them to benefit from digital learning and participate in the public debate” (European Commission 2011). This chapter will explicate the concepts of command-and-control regulation, self-regulation and co-regulation and discuss the suitability of these regulatory approaches to achieving the public policy objectives of creating a safer and better internet for children and of shielding children (and empowering children to shield themselves) from risk of harm.

Command-and-Control Regulation

Command-and-control regulation – also known as ‘classical’ or ‘traditional’ regulation – involves “state promulgation of legal rules prohibiting specified conduct underpinned by coercive sanctions (either civil or criminal in nature) if the prohibition is violated” (Morgan and Yeung 2007). The ultimate illustration of command-and-control regulation, then, is legislation; legal rules enshrined in statute and enforced by the state. Inherent in this construction of regulation are three distinct assumptions, all of which are being increasingly questioned by regulatory scholars: (1) the state is best positioned to enunciate community goals; (2) the state possesses the final authority; and (3) rules handed down in the form of commands are the primary means of sculpting citizens’ behaviour (Morgan and Yeung 2007).

Regulation in general and regulation within the media sector in particular has to face the fact that new technologies and internationalization have led to widespread and fundamental changes. […] Traditional regulation, though successful and efficient in the past, might be unsuitable under changed circumstances. The role of the state needs to be redefined. This is even true for fundamental objectives like the protection of minors. (Schulz and Held 2006: 49)

It is often contended that it is becoming increasingly difficult to rely on traditional regulation in today’s “complex and dynamic” audiovisual media environment – a converged environment in which the objective of regulation has shifted from one of protection to one of shared responsibility and empowerment (O’Neill and Barnes 2008). There are several reasons why command-and-control regulation might no longer constitute an appropriate approach when it comes to regulation of the audiovisual sector: (1) the role of the state as legislator,
enforcer and adjudicator means that there is little scope for outside input and influence and, in light of the assertion that the regulating state is increasingly suffering from a ‘knowledge gap’ (particularly when it comes to the regulation of technologically-complex, fast-changing sectors such as the audiovisual sector), collaboration between regulator and regulated is an increasingly crucial component of the regulatory process; (2) rigidity in the application of the law, an inherent feature of traditional regulation, means that command-and-control regulation is not conducive to creativity – essential for the continued development of the audiovisual sector and to ensure the competitiveness of the European audiovisual market; (3) the global nature of the audiovisual sector facilitates the circumvention of domestic regulations through “international forum-shopping” – a practice which involves ascertaining the jurisdiction with the most favourable legal regime for a particular activity and the anchoring of that activity within that particular regime (Lievens 2007; Schulz and Held 2006).

In short, the inherent characteristics of today’s converged media environment – “the international nature, technological qualities, and special architecture of the new networks” – arguably render traditional regulatory regimes unsuitable (Lievens, Dumortier and Ryan 2006).

The unsuitability of traditional regulation in this context is not a view universally shared. For example, according to Svantesson (2005), “descriptions of what characteristics of Internet communications challenge traditional models of regulation and governance” have a tendency to be “abstract and undeveloped”, with “surprisingly little efforts […] directed at analysing what makes the Internet different”. Characteristics aside, when it comes to the internet, proponents of traditional regulation (“regulatory traditionalists”) consider the state – the “pre-eminent existing governance agency” – to be the appropriate regulatory authority (Mayer-Schonberger 2002-2003). From a traditionalist perspective, the state is perceived as possessing “the democratic legitimisation, the procedural set-up, and the institutional enforcement to make regulations, including ones pertaining to cyberspace, work” (Mayer–Schonberger 2002-2003). Regulatory traditionalists, then, support state regulation of the internet on the basis that the state constitutes a legitimate source of law, and is possessed of the requisite authority to ensure enforcement of that law. Sceptics of the traditionalist position argue that conventional state regulation of the internet – a global network – diminishes the legitimacy normally associated with such regulation (Mayer-Schonberger 2002-2003). In other words, while the nation state is generally perceived as a legitimate source of regulatory authority when it comes to formulating, implementing and enforcing rules within and upon its own national constituency, this legitimacy is diminished when the nation state attempts to impose these rules outside its own national borders. Further, sceptics of the traditionalist viewpoint argue that the application and operation of a multitude of disparate national laws could give rise to a situation where internet users are bound by a plethora
of contrasting, indeed conflicting, regulations (Mayer-Schonberger 2002-2003). Regulatory traditionalists counter this claim by arguing that regulatory overlap is by no means unique to the realm of cyberspace, asserting that the conflict of laws doctrine was developed specifically to deal with the problem of “regulatory spillover” (Mayer-Schonberger 2002-2003). Opponents of the traditionalist perspective contend that a nation state’s enforcement powers do not hold sway in a global environment, while regulatory traditionalists counter that “perfect enforcement” of the law is not necessarily a prerequisite for a workable legal system in cyberspace (indeed, few areas of law can claim absolute enforcement) (Mayer-Schonberger 2002-2003). However, irrespective of whether or not “perfect enforcement” is an achievable objective, opponents of the traditionalist position point out that “sufficient enforcement” is a necessary element of any regulatory process (Mayer-Schonberger 2002-2003).

Traditional regulation, it is argued, fails to achieve an acceptable balance between competing rights and interests, for example, “the balance between the fundamental right of freedom of expression and the public-interest objective of protecting minors” (Lievens, Dumortier and Ryan 2006). Legislators, it is argued, encounter two primary difficulties when it comes to legislating for the protection of children from harmful media content using traditional regulatory mechanisms: (1) the potential for state-imposed restrictions to impinge upon adults’ freedom of expression rights (the “spillover effect”) and (2) the reality that at least some of the content from which the state seeks to protect children is constitutionally protected for adults (Saunders 2004). From the early to mid-1990s, the EU appeared to favour a conventional regulatory approach to internet regulation. The High-Level Group on the Information Society, in its report to the European Council in 1994, recommended “the establishment at the European level of an authority whose terms of reference will require prompt attention” (Bangemann Report 1994). Following on from the Bangemann Report, a 1994 Communication from the European Commission proposed a “broad regulatory framework package” encompassing market access, compatibility between networks, intellectual property rights and data protection (European Commission 1994). Additionally, in 1996, the European Parliament reiterated “the need for a European Regulatory Authority for communications regulation, and the promotion of standards at European and global level” (European Parliament 1996). According to Lievens (2007), when faced with the task of legislating for the regulation of content, governments have a tendency to lean towards censorship. Traditional regulation has been referred to as “the bluntest method” of prohibiting certain activities or types of speech, and the method with the “greatest incidental impact” in terms of its capacity to infringe upon the right to freedom of expression, particularly the freedom of expression rights of adults (Birnhack and Rowbottom 2004). As regards the role of the state in shielding children from the potentially deleterious effects of certain types of
media content, it is maintained that the state possesses an “independent interest” in the welfare of children residing within its jurisdiction (Archard 2004). The state also has what has been described as a “reproductive role” in ensuring that children develop the capacity to execute their responsibilities as citizens; possessing an “interest in securing over time the continued preconditions of its own future existence” (Archard 2004). In other words, children represent the future of any given society and, as such, the state possesses an obvious interest in ensuring that children develop into “capable, productive individuals” who are “able to play their part in democratic governance” (Vehmas 2009). It is also argued that the role of the state with regard to the protection of minors from conceivably harmful media content is primarily facilitative, supplementary to the role of the parent (Archard 2004).

**Alternative Regulatory Approaches:**
**The Rise of Self- and Co-Regulation**

The inadequacies of command-and-control regulation in conjunction with media convergence and the emergence of new information and communication technologies has prompted consideration of alternative regulatory mechanisms, mainly self- and co-regulation. While it is not always clear what exactly is meant by self- and co-regulation, both concepts are presented as alternatives and/or supplements to more traditional forms of regulation such as command-and-control regulation. In the context of European audiovisual media policy, self- and co-regulatory measures have been increasingly advocated from the late 1990s onwards.

**Self-Regulation**

Self-regulation is defined as the possibility for economic operators, the social partners, non-governmental organisations or associations to adopt amongst themselves and for themselves common guidelines at European level (particularly codes of practice or sectoral agreements).²

Put simply, the term self-regulation applies to the scenario wherein the industry concerned – as opposed to the state – assumes the role of legislator, enforcer and adjudicator (Campbell 1998-1999). Self-regulation is “often presented as the antithesis of law” but, in reality, it is extremely rare “for a regulatory system involving major conflicts between values to be unaccompanied by direct forms of legal rules and sanctions” (Prosser 2008). In other words, “pure self-regulation” (described as “processes of self-regulation where the state has no role to play”) is extremely unusual (Hans-Bredow Institut 2001). Industry self-regulation is sometimes referred to as “regulation by raised eyebrow” – a phrase used to
describe the practice whereby policymakers, expressing discontent about a particular issue, make ambiguous references to the possibility of legislative intervention thereby prompting the industry concerned to self-regulate (Jordan 2008; Dowd, Singer and Fretwell Wilson 2006). In other words, the threat of government intervention often serves as a trigger for industry self-regulation, or such threats are deliberately invoked by policymakers in order to incite industry to self-regulate.

There are several benefits and drawbacks associated with the concept of industry self-regulation (Campbell 1998-1999; Lievens 2007). It is contended that the majority of governments lack the requisite expertise (technical and otherwise) when it comes to regulating certain specialised sectors and that self-regulation, through its reliance on existing industry knowledge, allays such governmental shortcomings (Campbell 1998-1999). Further, it is argued that governments attempting to regulate particularised areas, such as the internet, inevitably find themselves “overloaded with work” and ultimately end up advocating industry self-regulation (Kleinsteuber 2003). It is arguably easier for the industry to revise its own rules in response to changing circumstances when it is not subject to the often rigorous procedural requirements of government (Campbell 1998-1999; Lievens 2007). The benefits of self-regulation include flexibility, the availability and use of industry expertise and the ability to react expeditiously to public concerns (Lievens 2007). Furthermore, it is suggested that industry members will more readily comply with regulations formulated from within as such rules are more likely to be perceived as reasonable (Campbell 1998-1999; Lievens 2007). In other words, the very concept of industry self-regulation serves to incentivise industry compliance.

On the other hand, sceptics of self-regulatory regimes assert that industry is more likely to utilise its expertise to further industry objectives and enhance profits rather than fulfil public policy objectives (Campbell 1998-1999). It is argued that, in the absence of some form of formal regulation, some industry players “will do nothing to prevent the distribution of harmful material, or children’s access thereto” (Birnhack and Rowbottom 2004). The very legitimacy of industry-produced codes of practice has been questioned on the basis that they lack sufficient transparency and accountability in both their formulation and general application (Kleinsteuber 2003). The inadequacy and difficulty of enforcement is commonly cited as the greatest weakness of self-regulation (Campbell 1998-1999; Lievens 2007). There is often reluctance on the part of the industry to commit adequate resources to the development and maintenance of an effective self-regulatory system and, as a result, the ability of an industry to carry out the role of enforcer is increasingly being questioned, as is its capacity to impose effective and meaningful sanctions for violations (Campbell 1998-1999). The self-regulatory approach has also been criticised for assigning too much responsibility to the private sector, a situation which could potentially
lead to a situation of “privatised governance”, in which certain key players within a particular industry begin to excessively influence, if not overwhelm, the regulatory process (Kleinsteuber 2003; Tambini, Leonardi and Marsden 2007).

The mid-to-late 1990s has been identified as the period during which the EU “quietly made a significant position change in its strategy for regulating the Internet market” (Feeley 1999). For example, the EU was supportive of the self-regulatory endeavours of the European Internet Service Providers Association (EuroISPA), established in 1997 (Feeley 1999). In addition, the Council of the EU’s 1998 Recommendation on the protection of minors and human dignity advocates the creation and implementation, at the Member State level, of a self-regulatory framework for the protection of minors and human dignity in the European audiovisual and information services industry (Council of the European Union 1998). The 1998 Recommendation expressly recognises the potential of self-regulation in providing the industry “with the means to adapt themselves rapidly to the quickening technical progress and to market globalisation”, further recognising that self-regulation has the necessary degree of flexibility to allow the industry to take account of rapid developments in this sector. However, despite this endorsement of self-regulation, the Recommendation makes it clear that self-regulation is perceived as a supplementary and/or complementary form of regulation – not as a substitute for “relevant regulatory frameworks at national and Community level.” In addition to endorsement at the EU level, the potential of self-regulation was also recognised by the Council of Europe (CoE) in its 1989 Recommendation concerning principles on the distribution of videograms having a violent, brutal or pornographic content (Council of Europe 1989). The stated objective of the Recommendation, issued some time before the proliferation of the internet and new media technologies, was to “protect minors against the pernicious influence of such videograms” and, to that end, the development of systems of self-regulation, such as industry codes of conduct and voluntary classification and control systems, was encouraged. Additionally, the CoE’s 1999 Declaration on a European policy for new information technologies makes express reference to self-regulation, and its 2001 Recommendation on self-regulation concerning cyber content encourages Member States to advocate the development of organisations “representative of Internet actors” and to encourage such organisations to formulate, implement and monitor regulatory mechanisms, such as codes of conduct, and “apply these standards, as far as possible,” to the ICT environment (Council of Europe 1999, 2001).

The EU continued to advocate the use of self-regulation in its 2002 Resolution on the labelling of certain video games and computer games according to age group and in its 2006 Recommendation on the protection of minors and human dignity – an updated version of its earlier 1998 Recommendation, referred to above (Council of the European Union 2002, 2006). However, it
is worth pointing out that, while the 2002 Resolution supports self-regulation both “on its own or as a complement to the measures implemented by Member States”, the 2006 Recommendation states that “self-regulation of the audiovisual sector is proving an effective additional measure, but is not sufficient to protect minors from messages with harmful content.” Furthermore, the 2006 Recommendation encourages the sharing of experience and best practice between existing self- and co-regulatory bodies, thereby emphasising the importance of co-operation, as well as placing an emphasis on the importance of assessing the effectiveness of self-regulatory approaches. The 2006 Recommendation, then, could be considered to be indicative of a palpable shift from self-regulation towards co-regulation (discussed below) (Lievens 2007). The EU’s 2007 European Framework for Safer Mobile Use by Teenagers and Children advocates “a framework-based approach to industry self-regulation” on the basis that such an approach is most suited to the “fast moving environment of mobile technology and services” (European Commission 2007).6 The 2007 Audiovisual Media Services Directive (AVMSD), codified in 2010 – a revision of the 1989 Television without Frontiers Directive, as amended in 1997 – calls on Member States to “recognise the role which effective self-regulation can play as a complement to the legislative and judicial and/or administrative mechanisms in place” (European Parliament and Council 2007). Like the 2006 Recommendation before it, the concepts of self- and co-regulation appear together in the Directive, with Member States being called upon to “encourage co-regulation and/or self-regulatory regimes at national level.” In addition, the Safer Social Networking Principles for the EU – voluntarily adopted by the industry in February 2009 – are part of the European Commission’s continued support for self-regulation on issues related to the safer use of the Internet by children (European Commission 2009).4 In its Agenda for Children’s Rights, the EU has once again affirmed its support for self-regulatory initiatives when it comes to the audiovisual sector (European Commission 2011). Specifically, the European Commission, acknowledging the self-regulatory endeavours of mobile service providers, social network service providers and the video games industry, states that it plans to “expand its call for action to manufacturers of mobile devices and game consoles, internet service providers, mobile applications”.

Co-Regulation

Co-regulation means the mechanism whereby a Community legislative act entrusts attainment of the objectives defined by the legislative authority to parties which are recognised in the field (such as economic operators, the social partners, non-governmental organisations, or associations).5

It has been argued that “faith in self-regulation is noticeably and steadily declining, and governments are tightening the reins in order to regain some control
over the regulatory process in fields where self-regulation has not been very efficient” (Lievens, Dumortier and Ryan, 2006). Moreover, “self-regulation of the Internet has recently been greatly criticized, due to problems of legitimacy and accountability, as well as concerns about private censorship and the protection of freedom of expression” (Lievens, Dumortier and Ryan 2006). There exist several – and diverse – interpretations of the exact meaning of co-regulation, resulting in an array of affiliated terminology, such as “two-tiered regulation”, “regulated self-regulation” and “audited self-regulation” (Lievens, Dumortier and Ryan 2006). It has been observed that, in recent years, the terms co-regulation and self-regulation increasingly appear together in European policy documents, often without clear distinction (Lievens, Dumortier and Ryan 2006). In fact, it is contended that there is no clear line between self- and co-regulation (Tam -bini, Leonardi, Danilo and Marsden 2008). Co-regulation has been described as including “a variety of different approaches within different countries and different sectors” and consisting “of more than just a combination of state regulation and self-regulation” (Schulz and Held 2006). Co-regulation manifests itself in numerous, and diverse, forms. The inexactness of the meaning of co-regulation – both as a concept and as a practice – need not be regarded as an impediment to its development but rather this ambiguity should be viewed as affording “much potential for milking” (McGonagle 2003). Furthermore, where a definition of co-regulation is offered, much still depends on whether said definition is construed in a broad or narrow sense (Lievens, Dumortier and Ryan 2006). The former European Commissioner for Information Society and Media, Viviane Reding, referred to a co-regulatory system as “one where public authorities accept that the protection of societal values can be left to self-regulatory mechanisms and codes of conduct, but where they reserve the right to step in in case that self-regulation should prove to be inefficient” (Reding 2006).

There are several benefits associated with co-regulation: all players are afforded the opportunity to participate in the regulatory process; a degree of pliability is injected into the regulatory process; the existence of a legislative safety net precipitates more effective enforcement; and co-regulation, as a regulatory practice, offers increased levels of accountability and transparency (Lievens 2007). Arguably, when the benefits and drawbacks of both traditional regulation and self-regulation are pitted alongside those of co-regulation, it becomes clear why increased endorsement of the latter “especially in the field of protection of minors against harmful content, seems appropriate and well-founded” (Lievens 2007). In the context of EU audiovisual policy, the EU’s 1998 Recommendation on the protection of minors and human dignity (discussed above) – despite the fact that the term co-regulation does not expressly appear in the Recommendation (and irrespective of multiple references to self-regulation) – is regarded by some as being co-regulatory in nature (Lievens, Dumortier
and Ryan 2006). In addition, the EU, in its 2006 Recommendation (discussed above) appears to favour an approach of “bottom-up harmonisation through cooperation between self-regulatory and co-regulatory bodies in the Member States” (Lievens 2007). Co-regulation also features in the EU’s 2007 Audiovisual Media Services Directive (AVMSD), which states that “[c]o-regulation gives, in its minimal form, a legal link between self-regulation and the national legislator in accordance with the legal traditions of the Member States” (AVMSD 2007). Further, the AVMSD provides that “[c]o-regulation should allow for the possibility of State intervention in the event of its objectives not being met.” The AVMSD requires Member States to ensure that content which “might seriously impair the physical, mental or moral development of minors” is only made available in ways which ensure children will not normally be able to access such content. The Directive, advocating both self-regulation and co-regulation, provides that “Member States shall encourage co- and/or self-regulatory regimes at national level in the fields coordinated by this Directive to the extent permitted by their legal systems.” Filtering technologies, content labelling and rating, and codes of conduct are all possible components of a co-regulatory regime. McGonagle (2003) cautions against becoming too embroiled in definitional exactitudes however, given that “regulatory policy is increasingly leaning towards co-regulation as a possible way of regulating media and protecting minors against harmful content”, these “terminological and conceptual pitfalls [...] must be addressed sooner rather than later” (Lievens, Dumortier and Ryan 2006).

Conclusion

The appropriateness of more traditional regulatory mechanisms when it comes to regulation of the ICT sector is a subject of on-going, and discordant, debate – and this will likely be the case for some time to come. There are a number of reasons why traditional regulation is not perhaps the most appropriate means of realising the objectives of achieving a better and safer internet for children and of protecting children from risk of harm. One major stumbling block is the fact that traditional regulation, in the form of legislation, tends to be reactive as opposed to prospective and, resultantly, will likely always lag behind technological advancements and developments. The reactive nature of legislation means that it can (and often does) quickly become ill-equipped – obsolete even – in dealing with the very issue it was designed to address. Another problematic aspect of legislation in this context is that its formulation necessarily involves subjection to the full rigours of the legislative process and all that this entails, meaning that such laws often take considerable time to come to fruition. These hurdles, in conjunction with rigidity and inflexibility (widely accepted as inherent characteristics of traditional regulation), make it
difficult to adapt traditional regulation to ‘fit’ the challenges presented by the ICT environment. Additionally, traditional regulation tends to be restrictive – prohibitive even – placing a negative obligation on its subjects not to engage in certain behaviours or activities. It is this aspect of regulation that is particularly difficult to reconcile with concepts like ‘empowerment’ and ‘participation’, concepts enshrined in the United Nations Convention on the Rights of the Child, as well as increasingly advocated at the European level by both the EU and the Council of Europe. While regulation, in the traditional sense, has not been entirely rejected as a means of achieving a safer and better internet for children, it is clear – at least at the EU level – that it is not the preferred approach of attaining this objective (European Commission 2012). However, despite this, it is clear that there will always be a place for – indeed a need for – more traditional forms of regulation in addressing issues like child sexual exploitation and abuse, child pornography and data protection, all of which are subject to EU law in the strict sense.

Sceptics of self-regulation often cite difficulties with implementation and enforcement as its single greatest weakness. This is a problem which has been acknowledged at the EU level, with the European Commission recently pointing to the need to provide structures for “independent monitoring” of self-regulatory regimes (European Commission 2012). To this end, the implementation of recent self-regulatory initiatives such as the European Framework for Safer Mobile Use by Younger Teenagers and Children (2007), the Safer Social Networking Principles for the EU (2009) and the Principles for the Safer Use of Connected Devices and Online Services by Children and Young People in the EU (2012) have all been placed under periodic review. For example, in June 2010, the signatories to the European Framework for Safer Mobile Use issued national implementation reports as part of the third implementation review of the initiative across the EU (GSMA 2011) and, in September 2011, the European Commission published the findings of a second independent assessment of the implementation of the Safer Social Networking Principles for the EU (European Commission 2011).

In addition, the European Commission in its report on the application of the 1998 and 2006 Recommendations on the protection of minors and human dignity (discussed above) referred to problems of inconsistency and ineffectiveness with regard to self-regulation. Specifically, the Commission stated that self-regulatory measures “quite often, […], lack ambition and consistency with similar measures put in place in other Member States, or they are simply not effectively implemented in practice” and, furthermore, stated that such inconsistency “can only lead to internal market fragmentation and to confusion for parents and teachers who try to identify the “do’s” and “don’ts” to protect and empower children who go online” (European Commission 2011). The Commission has, however, explicitly stated its preference for self-regulation over regulation in the traditional sense but also makes it clear that legislative
measures will be considered “if industry self-regulation fails to deliver” – more specifically, in its Communication on a European Strategy for a Better Internet for Children, the Commission states that it will consider legislative intervention where industry fails to deliver with regard to ensuring wider availability and use of parental controls, wider use of age rating and content classification, and ensuring the provision of simple and robust reporting tools for users (European Commission 2012). The Commission concludes that:

Ongoing effective industry self-regulation for the protection and empowerment of young people, with the appropriate benchmarks and independent monitoring systems in place, is needed to build trust in a sustainable and accountable governance model that could bring more flexible, timely and market-appropriate solutions than any regulatory initiatives. (European Commission 2012: 15)

Despite consistent and continued endorsement of self-regulation, there has, at the same time, been a move towards advocating it as part and parcel of a wider regulatory response to internet safety, as opposed to a regulatory response in and of itself. Given that the term co-regulation is capable of being applied to a wide range of regulatory combinations, and the fact that the line between self- and co-regulation is becoming increasingly blurred as these terms increasingly appear together, perhaps it is more apt to describe the current regulatory approach in this area as co-regulatory in nature.

Self-regulation, for the time being, retains its title as the most preferred regulatory approach for realising the objectives of creating a safer and better internet for children and of protecting them from risk of harm. However, the preference is not for self-regulation in its purest form and it is certainly not a case of laissez-faire; rather the preference is for a regulatory regime which is primarily self-regulatory yet is buttressed by other forms of regulation. Self-regulatory endeavours and initiatives in this context are under close scrutiny – legislative intervention will always lurk in the background, even if only to serve as a less than subtle means of incentivising industry compliance and enforcement.

Notes
1. According to regulatory traditionalists, while regulatory spillover effects in cyberspace might prove highly perplexing, such problems are not insurmountable. Traditionalists further contend that Internet users “fearing subjection to foreign rules” can, and with relative ease, employ technological methods in order to limit their interactions with foreign actors. However, this is undoubtedly a form of restriction – an undesirable concept in the context of Internet use. Opponents of regulatory traditionalists, cognisant of the undesirability of this situation, argue that the conflict of laws is conceptually intricate and, as such, the average Internet user cannot be expected to decipher such inherently complex legal concepts. Moreover, it is likely such an approach to Internet governance would seriously temper online behaviours, having a “chilling effect” and undermining “the very foundation of freedom of expression.”

3. See Chapter 6, this volume.

4. See Chapter 6, this volume.


6. See Chapter 1, this volume.

7. See Chapter 15, this volume.

8. See European Commission (2012) *European Strategy for a Better Internet for Children. COM(2012) 196 final*, p.2. “As highlighted in the Council Conclusions on the Protection of Children in the Digital World of 28 November 2011, a combination of policies is required to deliver a Better Internet for Children. Actions are being developed at the national, European or sectoral level. They need to be included in an EU-wide strategy, which develops baseline requirements and avoids fragmentation. *Regulation remains an option, but, where appropriate, it should preferably be avoided, in favour of more adaptable self-regulatory tools, and of education and empowerment.*” [Emphasis added]


References


Committee of Ministers of the Council of Europe (1989) *Recommendation (89)7 concerning principles on the distribution of videograms having a violent, brutal or pornographic content.*


Committee of Ministers of the Council of Europe (2001) *Recommendation (2001) 8 on self-regulation concerning cyber content (self-regulation and user protection against illegal or harmful content on new communications and information services).*


‘Knowledge Enhancement’

_The Risks and Opportunities of Evidence-based Policy_

Sonia Livingstone

Enhancing Knowledge

Knowledge enhancement projects are projects to strengthen the [Safer Internet] programme’s knowledge base on safer Internet and online technologies generally.¹

The EU Kids Online network has been funded by the European Commission’s (EC) Safer Internet programme since 2006 as a ‘knowledge enhancement’ project ‘to make a better internet for children.’² This goal is arguably more grounded in public values than the self-avowedly neo-liberal orientation of the EC’s Framework programmes (established to promote research that advances ‘the goals of growth, competitiveness and employment’).³ But being part of the Safer Internet programme rather than a regular Framework programme means that the network is one of very few research projects funded by a small organisation for which research was, at the start at least, a curious and rather tangential activity. In this chapter, I reflect on how the network has worked out what knowledge enhancement can mean, both for ourselves as academic researchers and for our funder and its active group of stakeholders across national governments, industry, law enforcement, children’s charities, educators and the public.

One early question was, what is the prior knowledge base to be enhanced through our work? A review of the available literature 10 years ago had identified very little research on children’s online opportunities and risks (Livingstone 2003). Even when we conducted our first review of the field a few years later, it was difficult to draw reliable conclusions from the few published studies – a couple of cross-national studies (notably, the SAFT project, Staksrud 2012; also the project, Mediappro 2006) and a scattering of national studies, mostly from the US. These used different definitions of internet use or risk, and different methods to sample and measure online experiences. Moreover, whatever was available in the academic field was largely unknown to practitioners, being written in academic prose and published in expensive academic journals. To
'enhance' knowledge, therefore, we first scoped what research existed, entering details of some 400 studies into a public database and also identifying key gaps in the evidence base (Staksrud, et al. 2007). But our task was not just one of identifying existing academic research and making it known to policymakers. As we soon realised, knowledge enhancement includes the need to explain about the nature of knowledge: we were repeatedly asked about the research process – the rationale behind sampling, the operationalisation of concepts, the problems of research ethics, the possibilities for analysis and interpretation. So for the first phase of EU Kids Online (2006-2009), we also promoted best practice in terms of method (see Lobe, et al. 2008), and developed a conceptual and comparative research framework (see Hasebrink, et al. 2009). Moreover, we found that knowledge enhancement was a two-way street, for we too had much to learn. After all, we found ourselves working with a stakeholder community experienced in the provision, management and evaluation of a wide range of awareness-raising and safety initiatives, with a wealth of expertise among them, even if not formally expressed or theorised in academic terms. Some of our knowledge enhancement efforts therefore enabled recognition and reflexivity more than enlightenment. We offered accounts of the world that were already familiar to practitioners, and pinpointed gaps in knowledge that had already been identified, if not always articulated.

The conduct and dissemination of our 2010 survey of 1,000 children aged 9-16 in each of 25 countries marked a step-change in terms of our capacity for knowledge enhancement. Now the focus was on generating new knowledge – notably, that obtained from interviewing children directly, rather than relying on accounts of their experience provided by parents or teachers – and ensuring this knowledge reached the ears of those who needed it. Fortunately for us (and perhaps unusually in public policy domains), we had an eager audience of policymakers (and the media) keen to learn of available findings, full of questions and suggestions, and ready to translate evidence-based recommendations into practice. Our reported percentages of children doing or experiencing x, y or z were seized upon as significant additions to the evidence base and, often as the legitimation for a particular policy direction or new safety initiative. For example, the finding that 38% of internet users aged 9-12 have a profile on a social networking site (SNS) (although many networks set a minimum joining age of 13) was widely cited as evidence of the failure of industry self-regulation. For the EC, the finding that the youngest children were least satisfied with online content provision (only one in three thought provision was ‘very good’) provoked them to initiate a pan-European prize for content produced for (and by) children. In the UK, the finding that 54% of parents say that they block or filter websites at home – putting them at the top of the European ranking – was much cited as evidence for Britain’s success.
in the internet safety league, although it was also used to encourage efforts to get the other half to use filtering software. Many other examples could be given, each country being most interested in instances where it ranked top or bottom within Europe.

Engaging in Debates

Enhancing knowledge may seem a rather calm and sensible affair, notwithstanding its challenges. But not all knowledge enhancement activities are straightforward, and one of the most challenging proved to be less the provision of ‘facts and figures’ but the management of their interpretation and use. There is little point, we discovered, in publishing findings and placing them on a library shelf or website: findings only enhance knowledge if they are used, and research users have particular and at times conflicting interests at stake. Thus knowledge enhancement required us to address the strongly felt anxieties and misconceptions about children’s internet use among not only policymakers but also the general public and the mass media. Especially in the absence of evidence, both experts and the wider public tend to endorse the popular trope of child-as-victim/internet-as-dangerous that has long characterised each new medium in the history of culture and technology (Critcher 2008). In part, this is an effect of the moral panic framing promoted by the tabloid media (Ponte, Bauwens, and Mascheroni 2009). But in part, the policy domain itself seemed to demand this – only problems attract attention and funding, so children’s internet use had to be framed as a problem if it was to be resourced (and as we ourselves found, when publishing our work, press releases without a sense of urgency or threat result in little publicity).

In effect, we found ourselves trying to change the dominant discourses regarding children’s internet use. To enhance knowledge, what people already know, or think they know, or prefer to believe about the world, must itself be brought into the open, challenged and rethought. All this led us into some heavily contested terrain. If we think back to the early days of mass access to the internet, just a decade or so ago, it was widely feared that the internet represented a virtual Wild West, a realm separate from the online world in both its content (being full of pornography and paedophiles) and its structure (being mysterious to adults in its workings and evading all regulation). Public pronouncements in the media, government and everyday discourse were (and still are) supremely technologically determinist in their vision of the internet landing fully formed in our lives as if an extra-terrestrial invader, although they were (and still are) also deeply familiar in their echoing of the moral panics that have always accompanied new media, especially those favoured by children. In this discourse, the internet represents a threat to innocence, a corrupter of
morals, undermining authority and damaging children’s intellectual and social development. These public anxieties enter into the regulatory debates among stakeholders by creating a sense of urgency regarding the supposedly imminent threat to children that skews the debate against cautious, complex or contingent judgements (Livingstone 2009).

The contrary position is almost as problematic. As critics became concerned that public fears about child online safety would stimulate ill-judged legislation to restrict both users and producers online – and both, it is true, occurred during the 1990s – an oppositional view emerged, claiming that children have all the digital skills they need to cope online, that parents, not industry, should be held responsible for their safety, and that regulatory efforts to improve safety represent covert or even overt moves towards censorship (according to speech rights advocates) and/or bureaucratic restrictions on market freedoms (according to the neo-liberals). As two critical scholars commented of the 2008 Internet Governance Forum, ‘the push for online child protection was perceived to be a threat to privacy and freedom of expression rights’ (Raboy and Shtern 2010: 219). Szoka and Thierer (2009:1) put it even more starkly, ‘Online privacy, child safety, free speech and anonymity are on a collision course.’ Yet on reflection, at least the advocates of children’s safety and of adult freedom of speech – if they must be pitched one against the other – are generally ready to argue the merits of their cases in public, and each side can and does respect the evidence (Livingstone 2011; Powell and Hills 2010). More difficult is addressing children’s safety insofar as it seems to call for more public intervention in the market, for here the opposition is not expressed in terms of values or evidence but rather in terms of feasibility (child safety proposals are judged impractical in a fast-paced, globalised market with a long and ill-coordinated value chain from provider to end-user). To penetrate the weaknesses in this position demands considerable insider knowledge of the technological, legal and business issues at stake.

In the context of hotly contested multi-stakeholder debates, finding space for calm voices, non-aligned positions and complex perspectives can be difficult (Hintz 2007). Certainly the contestation surrounding children’s internet safety made for a heady context in which to report, for example, that children encounter more or less risk, have more or fewer digital skills, or benefit from more or less attentive parenting. Any report, it seemed, had the potential to position us, perhaps misunderstand us, as being aligned with one or another group of stakeholders in an oppositional debate. The nature of the knowledge we produced, its relation to the contested debates that contextualised it and the ways in which we communicated it were all important in ensuring that EU Kids Online supported evidence-based policymaking rather than what has been cynically termed ‘policy-based evidence making’.
What Knowledge?

As anyone working in the field of research use knows, a central irony is the only limited extent to which evidence advocates can themselves draw on a robust evidence base to support their convictions that greater evidence use will ultimately be beneficial to public services. (Nutley, Walter, and Davies 2007: 271)

At the end of the first phase of our work, EU Kids Online had identified not only the range of crucial evidence gaps but also the array of methodological flaws that characterised them, further undermining the potential for grounding policymaking in evidence. Our bluff was called, however, when the EC Safer Internet programme funded our second phase of work precisely to fill those gaps using methods of our own design. The result was our conduct of a survey that combined both breadth and depth, hugely adding to the evidence base although greatly taxing the energies and expertise of the network. Nonetheless, as we became painfully aware, our ‘ideal project’ faced its own limitations, some more serious than others, and one of which was that its findings would seemingly go out of date sooner than we had managed to analyse and report them. Still, our efforts produced the most comprehensive, robust and complex dataset produced to date, and we were determined to mine its value for all its worth.

What knowledge did we have to communicate? When we began our work in 2006, these challenges – of the pace of change, of cultural differences, of being misunderstood or co-opted by the hotly contested rhetoric of moral anxieties versus deregulation (of markets, of speech) – seemed to impede the investigation of how children were using the internet and with what risk of harm. But in retrospect, it seems that the hazards that threatened to trip us up also proved useful in shaping our eventual direction. In other words, the very task of identifying, anticipating, contending with and/or avoiding these hazards provided a series of correctives that guided EU Kids Online towards working out, constructively, what knowledge was needed, what misconceptions could valuably be corrected and what argumentation would be most eagerly adopted.

Thus knowledge enhancement, we discovered, is best managed through a dialogic process of engagement between researchers and research users (widely defined to include all stakeholders from funders and experts to the public and the media). The framing and presentation of research findings is never purely descriptive – most obviously the headline of the press release, but also the terminology selected for the body of a report, the priorities embedded in the executive summary, each decision taken regarding what to include, highlight or omit, even the smallest words used to describe findings (as in, ‘only’ 17% of children experienced this or that) – all reveal the values of the researchers and their expectations of the policy process, and each is open to contestation. The same is true, of course, in designing and conducting a project in the first place.
With these cautions in mind, let us review the main knowledge contribution offered by EU Kids Online. The many findings of the 25-country survey have been amply detailed in other chapters in this volume and, even more so, in our recent book of research findings (Livingstone, Haddon and Görzig 2012), itself drawing on a series of reports and journal publications (see www.eukidsonline.net). Although these amount to hundreds of pages, with many tables and figures, we are often given just 10-15 minutes to distil the main findings into a short presentation, whether for academic or policy audiences; journalists, of course, reduce this further to a mere sound bite. So although each talk or report is differently tailored to its topic and audience, Table 1 distils our contribution into five points which have emerged through a dialogic and dialectic process of trial and error – trying out ideas in policy presentations, discovering the assumptions of others or the misunderstanding of our own work and then refining our presentation and re-analysing data until a stable synthesis could be reached that appears, over time, to have hit its mark with some success.

(Mis)communicating Knowledge

Young exposed to pornography. (The Daily Telegraph, 10 January 2011)
Net censors use UK’s kid-safety frenzy to justify clampdown. (The Register, 10 February 2011)

Some messages are particularly difficult to communicate, and framing their dissemination illustrates the wider challenge of (mis)communicating knowledge. For example, our finding that efforts to improve digital skills appear to increase not only the opportunities but also the risks can easily be (mis)read as undermining efforts to promote digital literacy. Problematic for EC and national governments promoting a self-regulatory approach is the finding that end-user filters do not seem to reduce children’s incidence of online risk. Another finding – this time not what industry wished to learn – is that 38% of 9- to 12-year-olds have SNS profiles that supposedly restrict such services to those aged 13+. These latter instances suggest that regulation – if its intent is to filter inappropriate content or enforce age-verification – is not really working and this, in turn, caused some concern within the EU Kids Online network; those endorsing a child rights perspective may not wish, even by implication, to support the rationale for further top-down, state-led regulation.

When the research topic is of widespread public as well as policy interest, the task of communicating knowledge is yet more difficult. Indeed, the considerable public anxiety surrounding children and online risk, amplified by tabloid media reporting, puts pressure on both researchers and policymakers to manage public scrutiny of their mutual negotiation as well as scrutiny of the evidence base and its use in policymaking. In an effort to present empirical findings in
Children are agents living in a world largely not of their own making. Although the internet is thoroughly embedded in their lives, with more privatised and mobile access, children are neither wholly media-savvy in their ability to deal with the digital environment nor simply victims, lacking resources to cope with whatever occurs to them online. Rather, they play a range of roles in relation to online content, contact and conduct (as recipient, participant, actor), and their prior experiences (online and offline) affect their internet use; moreover, the affordances of particular online sites as well as the support of teachers, parents and peers, all play a role. However, contra technologically determinist views, the internet may amplify, intensify or undermine benefits and harms, but should not be conceived as their sole or main cause.

Using the internet affords children both opportunities and risks and the two go hand in hand. Efforts to manage risk can have the unintended consequence of reducing opportunities, itself problematic given how few children as yet benefit from a deep or wide engagement with the internet. It is inappropriate to promote online opportunities with no thought to the consequences for risk; nor can restrictions be implemented to reduce risk without thinking of the possible costs to children’s online opportunities. Moreover, children seek out a range of ‘risky opportunities’.

<table>
<thead>
<tr>
<th>Key contribution</th>
<th>Supporting evidence</th>
<th>Use by policymakers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Children are agents living in a world largely not of their own making.</td>
<td>• Findings on digital literacies and skills</td>
<td>• Classification of risks widely cited to clarify the public policy agenda and to escape the tabloid agenda of internet-related fears</td>
</tr>
<tr>
<td></td>
<td>• Analysis of how far different children progress up the ‘ladder of opportunities’</td>
<td>• Relative lack of digital skills cited to stimulate both increased awareness-raising and educational efforts and to urge better designed interfaces (to ease children’s management of privacy, information and disclosure)</td>
</tr>
<tr>
<td></td>
<td>• Findings on a range of coping responses to different risks</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The classification of risks (as both a conceptual framework and in terms of evidence for each risk)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Findings on strategies and extent of mediation of internet use by teachers, parents and peers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Multivariate analyses predicting children’s online use, activities, risks, safety and harm</td>
<td></td>
</tr>
<tr>
<td>Using the internet affords children both opportunities and risks and the two go hand in hand. Efforts to manage risk can have the unintended consequence of reducing opportunities, itself problematic given how few children as yet benefit from a deep or wide engagement with the internet. It is inappropriate to promote online opportunities with no thought to the consequences for risk; nor can restrictions be implemented to reduce risk without thinking of the possible costs to children’s online opportunities. Moreover, children seek out a range of ‘risky opportunities’.</td>
<td>• Findings on the positive correlations among online activities, skills and risks as well as our typology of user types integrating these factors</td>
<td>• Awareness-raisers’ recognition that opportunities bring risks, and that risk management may restrict opportunities</td>
</tr>
<tr>
<td></td>
<td>• Analysis that restrictive parental mediation reduces skills and activities as well as risks</td>
<td>• EC established a pan-European prize for positive content produced by children and adults</td>
</tr>
<tr>
<td></td>
<td>• Findings on less-than-expected satisfaction among children with the online offer</td>
<td>• Acknowledgement of children’s experience – between risk and opportunity</td>
</tr>
<tr>
<td></td>
<td>• Findings on risky opportunities (meeting new people, displaying personal information online or pretending to be different on than offline)</td>
<td></td>
</tr>
<tr>
<td>Key contribution</td>
<td>Supporting evidence</td>
<td>Use by policymakers</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td><strong>Risk refers to the statistical probability (not inevitability) of harm and so is not inherently bad.</strong> The risks that upset children are not the same as those that worry adults. Risk and harm are explained differently and should not be confused. Offline and online risk factors make some children particularly vulnerable. Within the rise of user-generated content, some perpetrate as well as suffer online harm and these groups of children overlap. Last, a world without any risk at all is surely undesirable, as children must learn to face the unexpected, to take some degree of calculated risks and, within reason, to cope when things go wrong if children are to become resilient.</td>
<td><strong>Lower-than-expected findings for incidence of risk online</strong> (findings counter moral panics and reveal many children face little risk, and report even less harm from risk encounters)</td>
<td><strong>Efforts to avoid risk-averse, over-protective strategies</strong></td>
</tr>
<tr>
<td><strong>Individual, domestic and cross-cultural factors all shape children’s online experiences.</strong> At the level of the individual, age is the main factor differentiating children’s experiences; next most influential is whether they have psychological difficulties or are risk-takers. Parental use of and familiarity with the internet seems to matter more than socio-economic status (SES), and parental active mediation (more than restrictive or safety-focused mediation) improves children’s online experience. The incidence of online risk varies widely across countries, being greater in countries with higher GDP (because more use), while children’s digital skills are higher in countries with more schooling and more computers in classrooms. We propose a four-fold country classification: ‘lower use, lower risk’, ‘lower use, some risk’, ‘higher use, some risk’ and ‘higher use, higher risk’.</td>
<td><strong>Findings on individual differences in the incidence of online risk</strong></td>
<td><strong>Recognition of complex relation between child victims and (child or adult) perpetrators</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Findings on parental mediation, as perceived by parents and by children, and analyses of its effectiveness</strong></td>
<td><strong>Specific focus on varieties of vulnerability, to tailor advice and support appropriately</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Cross-cultural findings on similarities and differences in children’s online experiences</strong></td>
<td><strong>EC commissioned new research into online victims</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Analyses predicting cross-cultural differences by a range of external indicators</strong></td>
<td></td>
</tr>
</tbody>
</table>
Table 1.  Cont.

<table>
<thead>
<tr>
<th>Key contribution</th>
<th>Supporting evidence</th>
<th>Use by policymakers</th>
</tr>
</thead>
</table>
| More and more effective multi-stakeholder interventions are needed ‘to make the internet a better place for kids,’ in the words of EC Vice President, Neelie Kroes. Although our findings do not support the moral panics that the internet is a bad place for children, they do pinpoint diverse ways in which the design of online services (e.g. SNS) and their safety features (e.g. reporting tools, parental controls) can be improved. The findings also suggest more and less successful parental mediation strategies, as well as ways in which teachers and others who work with children can provide more effective awareness-raising and support to empower youth, prevent harm and improve safety and digital citizenship. | • Findings on use, skills and risk related to specific platforms (social networking, instant messaging, email, etc.)  
• Analysis of children’s SNS use in terms of age, anonymity, privacy, personal disclosure, etc.  
• Analysis of the partial take-up of parental controls, reporting tools and other technical provisions | • Debate over policy regarding ‘under-age’ SNS users  
• Wider array of parental mediation strategies advised than just restriction/filters  
• CEO coalition advised on better design of safety tools for use by children online |
a politically independent and scientifically rigorous manner, EU Kids Online has learned to pay particular attention to the process and genres of dissemination (the executive summary, press release, media report, YouTube interview or myth-busting blog post) as well as, of course, the academic journal article. The traditional academic view that knowledge is best enhanced by publishing new ideas and findings in peer-reviewed journals is far from that recognised by stakeholders; for the latter, by contrast, the purpose is to enhance the practical knowledge of those working ‘on the ground’ – the awareness-raisers, teachers, child protection workforce and those charged with customer care in industry. Moreover, while academics tend to begin with a simple problem statement and identify a complex, qualified and contingent answer, policymakers, by contrast, being faced with the messy realities of everyday life, listen out for simple, straightforward and actionable recommendations (notwithstanding their constant refrain that there is no ‘one-size-fits-all’ or ‘silver bullet’ solution). Hence they tend to filter our lengthy and detailed presentations in order to locate a single magic finding that may give them what they need. Retaining some control over this key bullet point or recommendation is crucial for the researcher.

Although producing the evidence base was crucial to our knowledge enhancement task, so, too, was negotiating the significance of that evidence base with stakeholders. Misconceptions about methodology turn out to be rife among policymakers and wider industry and civil society stakeholders with a smattering of social science knowledge: quick online polls that ‘contradicted’ our representative survey results were preferred over our findings; some were frustrated that we hadn’t asked children what we saw as unethical questions; and there were many confusions about sampling, about average differences not being absolute differences (a statistically significant difference can be small in terms of its effect size) and about whether correlation implies causation. Most worrying for the network was the tendency in public reporting to lose vital statistical information – for example, ‘72% of internet-using children aged 9-16’ quickly became ‘72% of children’, while ‘boys claim higher digital skills than girls’ turned into ‘girls lack digital skills’. Worst was the transformation of a complex finding (‘12% of internet-using 9- to 16-year-olds have seen sexual images online’ and of those, ‘one third were upset by the experience’) into a simple and incorrect one (‘one in three kids upset by online porn!’).

Merely publishing and publicising reports turned out to be insufficient – network members should ideally be personally present at any and all opportunities to disseminate, clarifying and contextualising the interpretation of findings and contesting misreadings as they occur among key policy actors. For example, we have to ‘be there’ to contest the (common) interpretation that reporting that some children are upset by online pornography is somehow a coded call for internet censorship. Or that showing that some parents can and do install filters is insufficient justification for the industry to consider regula-
tion unnecessary. Similarly, as we have found ourselves repeating over and over, reporting the percentage of children who encounter online risk is not the same as saying that that percentage of children is harmed by internet use. This last point has been the hardest to communicate, and the EU Kids Online network has become adept at putting over each point with great care, stating that risk refers to the statistical probability, not the inevitability of harm and, as the evidence suggests, a rather low probability at that; judging the probability of an event is different from calling it ‘probable’. Further, we emphasise that to talk of some children does not imply all children, that content is not in and of itself harmful (although it may be potentially harmful), as harm depends on the circumstances, that evidence of harm need not imply a severe or debilitating degree of harm, and also crucial, that talk of online risk does not mean we have forgotten that the internet has many benefits.

We have learned, therefore, to frame the presentation of our findings in ways that ensure the main points – concepts, findings and recommendations – are not only clear but that they are presented in such a way as to positively refute undesirable misreadings. As the five core conclusions in Table 1 illustrate, we now try not only to say what we want to say but also to counter particular claims that others have, until that point, explicitly or implicitly endorsed. In short, we have adapted our style of presentation to the discursive norms of policymakers (no jargon or statistics, short sentences and no circumlocution, start rather than end with the main point, etc.) the better to support the independence of our content (directly state and counter key claims, maintain integrity with your theoretical stance, stay close to your data, report contrary and unclear as well as supporting findings). Interestingly then, communicating knowledge demands attention to the argumentation unfolding among stakeholders, and this is fraught both because of the divergent (and often opaque) interests at stake and also because of the relentless timetable of policymaking and policy actions. But figuring out this timetable, learning to anticipate the policy windows of opportunity and dropping ongoing university commitments to ‘be there’ is demanding for academics used to longer-term planning cycles.  

Reflections on Evidence-based Policy

There is nothing a Government hates more than to be well-informed; for it makes the process of arriving at decisions much more complicated and difficult. (John Maynard Keynes, The Times, 11 March 1937)

Notwithstanding Keynes’ insight, the adoption of an evidence-based approach to policy represents a broad response among Western democracies to the pressing challenge of how to regulate increasingly globalised industries operating in a
highly specialised domain; it also meets the increasingly popular demand for a participatory rather than a top-down, command-and-control style of regulation. Thus we have seen across diverse regulatory domains the formation of multi-stakeholder alliances at supra- and sub-national as well as national levels that use research evidence on the one hand, to exploit expertise so as to be targeted and flexible and on the other hand, to draw ‘ordinary voices’ into complex and more inclusive processes of deliberation (Lunt and Livingstone 2012). Evidence, it is often held, provides a rational basis upon which policymakers can identify the problems requiring public policy intervention, inform the objectives that public policy can reasonably be expected to deliver, evaluate the effectiveness of policies once implemented and guide the process of policy adjustment and improvement (Sanderson 2002).

But producing evidence to underpin evidence-based policy is far from straightforward. For the EU Kids Online network, this has required, on the one hand, building interest and capacity among an initially disparate group of researchers across different countries and, on the other, building understanding among the Commission, national and international stakeholders and researchers, about what evidence is, how it should be interpreted and valued and how it may or may not guide practical policy initiatives. Both tasks are demanding, but at least the former – building research networks expert in a particular domain, often drawing on and debating diverse expertise and disciplinary perspectives, and working to create and sustain capacity – is already familiar to researchers. Yes, it makes their mutual differences salient, but the benefits of cooperating and complementing each other and of scaling-up the impact of their work are self-evident. The latter task is less familiar to many on both sides, not because academics live in ivory towers – on the contrary, they are fascinated by the complex reality of people’s lives and are often highly motivated to find solutions to real-world problems (Nyre 2009) – but because direct policy engagement is rarely what academics are trained or rewarded for, and because academia is littered with cautionary tales of policy efforts gone wrong. Indeed, the possibility that their ideas will be ignored, misunderstood, unwelcome and/or misused is enough to keep many academics from taking even a step outside the university, even though there is, as we have also discovered, much to learn and much to gain from such direct engagement.

Academics conducting research to inform policy are faced with a paradox that requires careful and reflexive navigation. On the one hand, we know that research is value-laden, always conducted from a particular standpoint, preferably aware of its possible consequences – in short, an intervention in the policy space in its own right. Yet on the other hand, policymakers value research only insofar as it sustains the claim to objectivity and independence. In other words, it is precisely our disinterestedness that gives us the right to contribute and comment in a policy debate where interests conflict. In relation
to the politics of knowledge, this point has been much discussed: Sanderson (2002: 6) observes, following the constructivist position (e.g. Guba and Lincoln 1994), ‘that scientific knowledge can have no unique claim to objectivity, and that research does not simply inform policy development in an instrumental way but rather plays an important role in promoting broader “enlightenment” of policy makers’ by engaging in a deliberative process with them. While this captures, in practice, the spirit of the process that EU Kids Online has engaged with, it is the claim of objective knowledge that has rhetorical power beyond the academy, leaving the paradox unresolved.

The inevitability of a standpoint, I suggest, need not undermine the value of our evidence or arguments; rather, policy and public audiences should be in receipt of knowledge about us and our work to evaluate them fairly. It is important that EU Kids Online works independently of governmental, charitable and industry interests and that it strives to meet the exacting standards of the academic community, which it does by making its methodology transparent, its data available and its analyses open to critical peer review. Nonetheless, our particular politics and values inevitably direct the choices made in our research, and these have been the subject of much discussion within the network. A major priority, early agreed upon, was to frame the work of EU Kids Online within the United Nations Convention on the Rights of the Child (Hamelink 2008). This has meant foregrounding children’s experiences and perceptions, adopting a child-centred methodology insofar as possible and advocating for children’s rights when these need re-affirming – they are easily lost, for instance, in the struggle between child protectionists and the free (adult) speech lobby (Livingstone 2011). But more dialogically, given that we are always addressing a particular audience (industry, child protection, government, parents, and so forth), we found it a good rule of thumb to question the assumptions and conclusions of each particular audience: for example, industry can be challenged if it hopes to rely on parents for child protection, but parents can be challenged to step up when they expect governments to manage the internet for their children. Since our findings provide qualified support for the safety contributions of each of a range of stakeholders, this strategy is consistent with both the evidence and our independence from the audience being addressed.

Let me conclude by observing, with Nutley, et al. (2007), that there is more than one model of evidence-based policy making in circulation. The ‘push’ model typically favoured by academics – according to which knowledge is disseminated to policymakers in the form and at the time that suits academics – is of limited value, since academic writing is not only little understood but is easily misunderstood, and it easily misses its mark. The ‘pull’ model, by contrast, is often experienced as unduly onerous by academics: in this problem-solving model, policymakers seek out research findings to address a specific question or problem, but of course academics are rarely at leisure to answer the question with
the urgency expected of them, and so both sides are often frustrated. Both push and pull models, although the most obvious, suffer the limitations consequent upon the typically poor relations sustained between academics and policymakers; if neither knows how the other works, of the nature of their concerns and the demands upon them, then their interactions are likely to prove frustrating.

Worse still are Nutley, et al.’s next two models. The political model uses research findings as ammunition when decision-making is adversarial. The tactical model treats research findings as a resource for applying or deflecting pressure, supporting or rejecting a decision, as desired (as discussed, for example, in Buckingham 2009). Both are sufficient to make academics run back to the ivory tower, preferring not to engage at all, to keep their knowledge to themselves, than to be thus abused. But as should be clear, EU Kids Online has sought a different approach, and here Nutley, et al.’s last two models are useful, representing in essence minimal and maximal versions of what is surely the optimal strategy. Specifically, the interactive model envisages a sustained interaction between researchers and policymakers, while the enlightenment model goes further, transcending the instrumental use of research by recognising that research is not a pre-given but is rather developed, interpreted and used within a dynamic and constructive process of engagement and mutual learning between researchers and policymakers. It must be confessed that, although EU Kids Online does in many ways aspire to this enlightenment model, it has taken a long time to build sufficient trust on either side to enable this, and any success remains fragile.

Although the long-term interests of researchers and policymakers appear aligned (that is, to make the world ‘a better place’ for children), not only may their short-term interests diverge (for example, taking the time to conduct careful research versus delivering results when a policy process requires them), but more importantly, their values remain distinct. Remaining reflexive about these differences is therefore crucial. Policymakers must determine what would make the world better for children (such as more positive online content, less harm or more effective industry self-regulation). Meanwhile, academic researchers must reserve the right always to question these determinations (what is ‘positive’, ‘better’ or ‘effective’?). Alliances can and should be only provisional, never comfortably established, with academics continually moving between the insider role (advising, negotiating, collaborating) and the outsider role (critiquing, doubting, rethinking) (Bohman 1991). Nutley, et al. (2007: 266) are optimistic, asserting that ‘there is real scope here for the creation and reinigoration of a variety of partnerships aimed at fostering a growth in research-informed dialogue.’ But more often, it seems that when such partnerships occur, they tend to be instrumental (Lunt and Livingstone 2012), lasting the duration of a project but perhaps not longer. To protect us all from complacency, and to keep us on our toes, I suggest that this is as it should be.
Notes
2. As announced by EC Vice President Neelie Kroes in establishing a coalition of chief executive officers (CEOs) of major internet companies on 1 December 2011; see http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/415&format=HTML&aged=0&language=EN&guiLanguage=en.
4. Since updated to include 1200+ studies, see http://www.lse.ac.uk/media@lse/research/EU-KidsOnline/DB/home.aspx. An image that captures research on children and the internet a decade or so ago is that of the Tower of Babel: when it comes to sharing knowledge across countries, language represents a serious barrier, too little recognised in our English-dominated research environment. Not only do researchers publish in national languages, but also because their research participants speak those languages, itself an especial concern in representing the experiences of children across Europe. Language differences are not eliminated by the (expensive) process of translation, for they reflect embedded cultural differences in meaning, value and distinction. This was brought home to the EU Kids Online network when we began discussing cyberbullying, a phenomenon newly being discussed in English language research but apparently unrecognised in many other languages or, at least, not named as such. The word ‘bully’ did not exist in some languages, and the nearest translation referred to harassment among adults in the workplace, ill-applied to children at school, although now the English word has taken hold in many languages.
5. Examples include the US 1996 Communications Decency Act (struck down in 1997) and the Child Online Protection Act (passed in 1998 to restrict children’s access to online pornography, and struck down as unconstitutional in 2009), as well as the Dot-Kids Implementation and Efficiency Act (passed in 2002 but never implemented and thus effectively defunct) (Livingstone, 2011).
6. Although EU Kids Online as a network lacked sufficient expertise in this regard, along with many working from a child rights and child protection perspective, the wider policy field has addressed this by building multi-stakeholder coalitions, most notably, the CEO coalition instigated by EC Vice President Neelie Kroes in 2011-12; in the UK, the UK Council for Child Internet Safety plays a similar role in ensuring informed collaboration across different interests.
7. For notwithstanding the oft-stated claim that this is a multi-stakeholder debate, in practice, participants found themselves aligned on one or other of two sides – industry versus non-governmental organisations (NGOs).
8. Of course we are not the only researchers producing knowledge in this field, and our work to develop communicable and useful findings has been conducted sometimes explicitly and sometimes tacitly in tandem with those in cognate fields or countries (e.g. Palfrey, et al., 2008; Smith, Mahdavi, and Carvalho, 2008; Ybarra, et al., 2007).
9. Our findings on parental mediation also threatened to undermine children’s right to enjoy the opportunities offered by the internet, since it turned out that children not only encounter fewer risks online if their parents restrict their internet use but they also reduce children’s online opportunities. So rather than promote the evidence-based policy recommendation that parents should restrict children’s internet use, we instead investigated whether any parental strategy effectively both reduces risks and increases opportunities. This proved a more complex question; our eventual answer – that if parents actively mediate their children’s internet use, they may reduce their child’s experience of harm without reducing their opportunities and digital skills – matched both the empirical findings and our child rights values (Duerager and Livingstone, 2012).
10. The question of timing is crucial – EU Kids Online cannot be the only research enterprise to have discovered that findings released when they become available (and certainly if one waits for the academic publication) easily miss their mark, whereas findings produced to fit a particular ‘policy window’ can reach a wide and relevant audience. A practical compromise, we have found, may be achieved by timing the release of findings according
to the policy calendar of stakeholder events, speeches and conferences (a calendar that is not written down anywhere in advance and takes effort as well as insider knowledge to construct).

11. Specifically, the EU Kids Online network has deliberately pursued a strategy of, first, making public as much as possible of the data (publishing the cross-tabulations immediately, lodging the full dataset in a public archive within a year of the fieldwork, producing a detailed report of findings as swiftly as possible); second, presenting the findings in themed short reports and presentations tailored to particular policy debates; and third, submitting its work to peer-reviewed academic journals and book publishers where, it may surprise policymakers to learn, the work faces a different set of critiques (regarding our theoretical framework, the supposedly excessive size of our sample and, especially, the selection and operationalisation of concepts – for example, digital skills – in terms of particular items and scales).

12. Practically, then, we emphasise children’s online ‘opportunities and risks’ rather than just the risks, and routinely report on the opportunities for learning, communication, sociality and fun that the internet can and should afford children before discussing the risks; moreover, we argue that some degree of exposure to some risks may even be beneficial, for only then can they become resilient and learn how to cope themselves with what they find online.

References


Chapter 6

Self-Regulation

Jos de Haan, Simone van der Hof,
Wim Bekkers & Remco Pijpers

The Relevance of Self-regulation

Since 2000, self-regulation has featured prominently as an element of the European Commission’s initiative to improve governance and as part of its Better Regulation agenda (European Commission 2001). The Interinstitutional Agreement on Better Law-Making defines self-regulation as: “The possibility for economic operators, the social partners, NGOs or associations to adopt amongst themselves, and for themselves, common guidelines at European level (particularly codes of practices or sectoral agreements)” (European Commission 2003). In many cases, self-regulation is combined with statutory regulation and this combination is referred to as co-regulation. In such situations, the development, implementation or enforcement of regulation is a joint responsibility of the state and the regulated organisation(s) (Bartle and Vass 2005) (for a more detailed discussion of the concepts self- and co-regulation see chapter 4, this volume).

In the present era of globalisation and deregulation, industry generally prefers self-regulation over statutory regulation because of the greater autonomy and freedom from state intervention it affords. Governments, at the same time, may also prefer self-regulation. Public officials often assume that industry practitioners have more expertise and technical knowledge. Utilisation of this knowledge and expertise leads, one assumes, to greater compliance and effectiveness since practical rules can be more easily developed, and also to greater efficiency because of lower costs of gathering information for the state. High compliance also results in more goodwill and loyalty (Ogus 1994; Balwin and Cave 1999). Besides issues of effectiveness and efficiency, public accountability and legitimacy also play a key role in the choice between self-regulation, statutory regulation or a combined form of co-regulation. For example, the legitimacy of codes of conduct (commonly cited as an example of industry self-regulation) has been questioned on the ground that they lack sufficient transparency and accountability in terms of their development, implementation and enforcement. On the other hand, self-regulation has advantages over no
regulation at all. Self-regulation may overcome market failures and prevent abuses. For example, without the counterbalance of self-regulation, industry players might violate economic or privacy interests of citizens. Self-regulatory schemes are intended to act in the public interest, not just the private interest. They should meet statutory objectives and apply effective systems and processes based on transparency and public accountability (Bartle and Vass 2005).

The rise of the internet raises new questions about regulation. With the fast pace of change in internet and mobile technologies, industry groups are themselves deemed to be best positioned to keep up with the latest technologies and trends of use (Cave, et al. 2008). Within the ICT sector, self-regulation has developed a rich variety of forms and tackled a wide range of policy concerns. In particular, the European Commission has favoured industry-led codes and agreements to deal with many issues of risk, safety, and child protection that have arisen (O’Neill and McLaughlin 2010).

Anglo-Saxon, Northern and Central European countries have a greater tradition of self-regulation than Latin and Southern European countries, where legislation has tended to play a a more important role. On-going work in Europe and elsewhere (FOSI 2008; AOL/NCSA 2004) includes efforts to ensure that risk and safety considerations are the focus of self-regulatory actions by industry. These efforts preceded the new proposal of the Safer Internet Programme (2009-2013) to co-fund projects to foster self-regulatory initiatives in this field and involve children in creating a safer online environment. Building on the first instalment of the Internet Action Plan (1999-2004) which supported self-regulation (e.g. the Internet Content Rating Association or ICRA in the field of content labelling), self- and co-regulatory initiatives are underway to address content labelling and trust marks, age verification, social networking, moderation of interactive services, managing mobile services, and so forth (PricewaterhouseCoopers 2009; European Commission 2009). These are particularly important for content that is not necessarily illegal but which, research suggests, can be harmful to children.

In this chapter, we discuss three cases of self-regulation related to the online safety of children, from which we draw conclusions about the strengths and weaknesses of self-regulation designed for this purpose. We also look at factors of commitment, compliance and effectiveness that might improve the quality of self-regulation. By commitment, we refer to the agreement or promise to comply with specific guidelines, specifications, or rules. This agreement cannot be enforced by legal sanctions but carries a moral pressure to comply. Compliance signifies a state of conforming to established guidelines, specifications, or rules. By effectiveness we mean the extent to which specific guidelines, specifications, or rules fulfil their intended purposes or functions.

In the first case, we discuss the operation of self-regulation in the world of computer games. PEGI, or Pan-European Game Information was introduced
in 2003 as an age classification system in European countries in order to help parents make informed decisions when purchasing computer games for their children. The second case concerns self-regulation guiding social networking services accessed by minors under principles coordinated by the European Commission and signed by all the major industry players (European Commission 2009). The third case deals with the European Framework for Safer Mobile Use by Young Teenagers and Children. This is an example of a self-regulatory agreement signed by mobile operators in 2007 and which formulated principles and measures that subscribers commit to implementing at a national level. Each of these cases is discussed from a European perspective (and includes illustrative practices from single countries where relevant). In each case, we address the following questions:

1. Why is self-regulation relevant (which purpose or function is it aimed at, and why is it preferred over other approaches)?

2. Which initiatives, guidelines, codes of conduct are specified and what do they contain?

3. How is it organised, in what form and how broadly is it supported?

4. How effective is each one of the self-regulatory regimes (considering that they may be organised in different ways and may serve different functions)?

5. What suggestions for improvement can be made?

**The PEGI/PEGI Online system**

PEGI (Pan-European Game Information)\(^1\) is the European classification and information system for games. The classification system was developed by ISFE (Interactive Software Federation of Europe), the European industry association of video games publishers, which was established in 1998 to represent the interests of the sector vis-à-vis the European Union and international institutions.\(^2\) Sony, Microsoft, Nintendo, Electronic Arts, Activision, Ubisoft and many other game companies are members of ISFE. The PEGI system is applied and accepted in all European countries, with Germany as the only exception.\(^3\) As of April 2003, nearly all console and PC games in Europe bear PEGI age ratings and content descriptors.

PEGI was designed to help parents make informed decisions about the content of games when purchasing them for their children. As stated by ISFE: “The system is part of the industry’s commitment to protect minors and to build trust with consumers by ensuring that information about video game content is provided in a responsible manner”.\(^4\) Age ratings and content descriptors
give an indication of the game content. There are five age classifications: 3, 7, 12, 16 and 18, and eight content descriptors for violence, fear, sex, drugs, bad language, gambling, discrimination and whether online gameplay is possible. The content descriptors indicate the elements of gameplay that led to its particular age rating.

Figure 1. The PEGI Age Ratings and Content Descriptors

The European Commission and national governments attach great value to PEGI, providing encouragement for what is seen as a successful example of strong corporate social responsibility. It does have some inherent limitations, however, and the set-up, implementation, monitoring and quality supervision of the scheme remain the industry’s responsibility. Despite this, a growing number of countries, including Finland, Iceland, Ireland, Israel, Lithuania, the Netherlands, the UK and part of Austria, support PEGI with national legislation of some description.

In some countries, PEGI is acknowledged alongside national age symbols for audio-visual media and enforced by the penal code (e.g. Finland and Lithuania), whereas in others, it is a requirement of consumer legislation (e.g. in the Netherlands and UK). It should be noted that the classification of games and compliance with retail enforcement laws are two different things; the fact that these laws exist does not make PEGI a less self-regulated system.

The foundations for PEGI were laid in May 2001 when representatives of the video game industry and national governments, scientists and rating experts, at the behest of the European Commission, met to discuss whether an international classification system for games was desirable or feasible. The fact that PEGI could be conceived in Brussels and born in Milan exactly one year later was a surprise. After all, national classification systems for games already existed. Though agreement about the desirability of a harmonised European system of game classification was widespread, there were strong doubts about the feasibility of such a system. In particular, the assumed cultural differences on potentially harmful content were considered to be problematic as well as
the fact that countries such as the UK would have to give up its own traditional games age rating bands, i.e. the UK’s domestic age ratings of 11 and 15 were substituted by PEGI 12 and 16 age ratings. The film industry had never succeeded in creating one. In May 2002, two task forces with representatives of all parties involved presented a proposal for a harmonised classification system, modelled on the Dutch “Kijkwijzer” system, established by the Netherlands Institute for the Classification of Audiovisual Media (NICAM), and on the Entertainment Leisure Software Publishers Association (ELSPA) system in the UK. Countries proved to be willing to make concessions to participate in PEGI, for example by giving up national age rating systems that had been in use for years. They were willing to put aside self-interest in favour of the public interest. Thus, the first PEGI classification system was accomplished in April 2003.

Commitment and Compliance

PEGI was designed to ensure maximum robustness for making recommendations to European consumers, especially parents, about the suitability of video game content. Each game publisher that joins PEGI must sign a Code of Conduct through which it commits to provide parents with objective, intelligible and reliable information regarding the suitability of a game’s content. By signing the Code, the publisher also aims to ensure consistency in the advertising of a product, and to refrain from putting products on the market likely to be in breach of human decency. The commitment to this Code is very high: more than 800 international game publishers have signed up to the system, meaning that PEGI is now used by all companies publishing games in Europe for PlayStation, Xbox, Wii, Nintendo DS, etc. As compliance to the Code of Conduct is also high, practically all games in Europe have, since 2003, been clearly labelled with age ratings and content descriptors. By the end of 2012, more than 20,000 games were classified by this system.

An important condition, crucial to PEGI’s success, is the attitude of the games industry, especially those prominent console manufacturers that operate on a global basis – Sony (Playstation), Microsoft (Xbox) and Nintendo (Wii) – who clearly desired a well-functioning European game classification system. Here, we see a convergence of the public interest and the self-interest of corporate social responsibility: as market-leaders, the three big companies were able to encourage games publishers to use the PEGI system.

A second factor in PEGI’s success is that its criteria for classifying games, the age ratings and the content descriptors, are uniform all over Europe. This was a real breakthrough: the UK, for example, gave up its own age ratings.

The third factor for success is the contribution of independent scientists with expertise in the field of gaming effects studies who, as part of the so-called PEGI Experts Group, give advice on the classification criteria.
Finally, a fourth success factor is the independent status of PEGI S.A., the organisation that manages the PEGI system on a day-to-day basis. Its representative committees also ensure broad participation: the PEGI Council is the independent advisory body consisting of representatives of currently 17 European countries’ governments. The Council gives national governments a voice in PEGI and keeps them informed about the evolution of the system. Other committees include the above mentioned PEGI Experts Group, the Complaints Board and the Enforcement Committee, which is an independent commission authorised to impose sanctions of up to €500,000.

This set-up leads to a self-regulating and flexible system, flexibility being an important criterion in the context of the game industry with its rapidly developing technology. A static system would risk collapse in a short period of time as a result of its own limitations. In recent years, the classification criteria have been adapted and improved several times. In addition, if one or more countries deem it necessary, it is possible to add a criterion as, for example, when an additional pictogram for “gambling” was added at Greece’s request.

The adaptations mentioned here are possible within the framework of self-regulation; PEGI S.A. makes its own decisions with the help of industry representatives and independent experts and in consultation with the PEGI Council. Given the near universal support given by the games industry to PEGI and its track record of success, it is understandable that self-regulation is preferred over more inflexible forms of regulation, such as legislation. PEGI was described by Commissioner Reding as “a good example of an industry initiative developed in co-operation with other stakeholders which allows a rapid and flexible solution to the problems of new technologies and greater safety for our children.”

All things considered, it is little surprise, then, that PEGI, as a uniform and effective system, has been hailed as a European success story.

**Effectiveness**

The effectiveness of PEGI is evidenced primarily in the satisfaction of its users. PEGI is valued by many people across Europe: 89% stated they found the age rating symbols useful (85% for the content descriptors), while 86% found their meaning clear (90% for the content descriptors) (Ipsos MediaCT 2012). PEGI’s experience shows that self-regulation can actually be effective if one or more dominant, leading parties in the sector are willing and able to enforce compliance with a certain form of self-regulation.

**Suggestions for Improvement**

More work is needed by PEGI to make its symbols more widely recognised throughout Europe. Substantial efforts are also required to make PEGI Online more successful. PEGI Online is an addition to the PEGI system and aims to
protect young people in Europe against inappropriate online game content as well as to teach parents how their children can play and stay safe online. In contrast to games published in a physical medium, online games are published on a platform without boundaries or any form of supervision by internet regulatory agencies. On the internet, there is no obligation for publishers of online games to show a classification: neither the government nor any internet regulatory authority can force them to do so. In order for PEGI Online to be more successful and meaningful, therefore, three conditions must be met:

- PEGI Online should offer added value to consumers;
- European and national governments should appeal to the corporate social responsibility of major online game publishers to apply PEGI Online;
- ISFE, as the international industry organisation, should take the lead in promoting the PEGI Online scheme.\(^8\)

Time will tell if meaningful self-regulation takes shape in this way. Marsden (2008a: 178) summarises the challenge like this: “A test for the PEGI Online system will be which non-European and online publishers choose to join and rate their games, given that there is no distributor physical bottleneck and the market to this point has been dominated by non-EU publishers.”

In recent years, the fast-growing popularity of mobile and online games has led to another development. The inherently global nature of the market for digitally delivered games forced PEGI and other rating boards across the globe to rethink the classification model. Although digital platforms often still have local storefronts, it became clear that digital publishers were in need of a different and more efficient approach to obtain age classifications for their products.

PEGI worked together with ESRB (United States), USK (Germany), ClassInd (Brazil), FPB (South Africa) and the Australian Classification Board to create IARC or International Age Rating Coalition. IARC combines the criteria of all participating rating boards into one big flowchart of questions. Based on the input to these questions, the publisher can get the appropriate age classification for every single region. IARC is set for launch at the end of 2013 and aims to include as much as possible of the digitally delivered content (games but also other apps) that is available to consumers in the participating countries.

**Safer Social Networking Principles for the EU**

In February 2009, major social networking service providers (SNS providers) in Europe adopted the Safer Social Networking Principles for the EU (SSNP).\(^9\) In light of children becoming more and more actively involved in publishing personal information on social media profiles, and being particularly vulnerable
in respect of encountering undesirable or upsetting experiences,\(^\text{10}\) it was felt necessary to coordinate efforts to improve protective measures at the source (i.e. within the services themselves). The guidelines had been discussed in the European Social Networking Task Force, organised by the European Commission, which – besides industry – also involved academics and child-welfare organisations. Basically, the principles are a hybrid form of self-regulation, given the involvement of the European Commission in initiating and evaluating the implementation of this regulatory initiative. Since the adoption of the principles by the industry is voluntary and, because there is no legislative force behind the principles, this is not a form of co-regulation (see Cave, et al. 2008).

For a variety of reasons, the European Commission considers industry pan-EU self-regulation as the preferred option for regulating online child safety on social networking sites. These reasons include the wide range of online risks for children, the constantly changing technological landscape, and the time-consuming process of bringing formal legislation of 27 member states up to speed with EU and international internet developments. Self-regulation is generally believed to allow more flexibility to address internet issues in a more timely and cost-efficient manner (Weber 2010). Moreover, through multi-stakeholder collaboration, online risks may be more effectively addressed (see Weber 2010). By involving stakeholders, an appeal can be made to their expertise and, moreover, to the commitment of the industry that is addressed by the principles. The principles must be seen in light of an ongoing dialogue on online child safety and the respective roles of other stakeholders, like parents, government, police, civil society and SNS users themselves. Hence, the principles are not an end in themselves and function as one mechanism amongst a myriad of responsibilities and initiatives.

The goal of the SNS principles is:

To provide good practice recommendations for the providers of social networking and other user interactive sites, to enhance the safety of children and young people using their services. (SSNP 2009: 1).

The principles thus provide platform-independent guidance on child-safety issues in online social networking which SNS providers can refer to, depending on the nature of the services and the levels of safety needed. All of these services, however, include a range of common features – i.e. social interaction, personal profiles or personal data disclosure, communication schemes, and search facilities – which raise similar safety issues. This implies that the principles basically apply to each SNS or interactive service. Nonetheless, the risks addressed by the principles can be quite diverse and include, amongst others, illegal or age-inappropriate content, inappropriate online sexual solicitation, and illegal, risky or anti-social behaviour. The various SNS providers’ risk-aversion strategies may, therefore, also vary.
The SSNP consist of seven principles outlining the responsibilities of SNS providers, which involve assessing their services and ensuring that potential risks for youth are prevented or mitigated. The list of principles is shown in Table 1.

**Table 1. Safer Social Networking Principles**

<table>
<thead>
<tr>
<th>Principle</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principle 1</td>
<td>Raise awareness of safety education messages and acceptable use policies to users, parents, teachers and carers in a prominent, clear and age-appropriate manner</td>
</tr>
<tr>
<td>Principle 2</td>
<td>Work towards ensuring that services are age-appropriate for the intended audience</td>
</tr>
<tr>
<td>Principle 3</td>
<td>Empower users through tools and technology</td>
</tr>
<tr>
<td>Principle 4</td>
<td>Provide easy-to-use mechanisms to report conduct or content that violates the Terms of Service</td>
</tr>
<tr>
<td>Principle 5</td>
<td>Respond to notifications of illegal content or conduct</td>
</tr>
<tr>
<td>Principle 6</td>
<td>Enable and encourage users to employ a safe approach to personal information and privacy</td>
</tr>
<tr>
<td>Principle 7</td>
<td>Assess the means for reviewing illegal or prohibited content/conduct</td>
</tr>
</tbody>
</table>

Based on these principles, the recommended safety strategies for SNS providers can be divided into five overall categories:

I. Safety policies or help pages – express guidance for users (including children and parents) on safe use or how to deal with safety problems;

II. Technological tools or mechanisms – age verification; parental controls; labelling/rating/age restrictions; content filters; restrictions on profile searchability; default settings to ensure maximum levels of privacy and protection; blocking/moderation/reporting controls;

III. Safety procedures – procedures for reporting misconduct and illegal or age-inappropriate content; links to emergency services or law enforcement; good-practice procedures for recruiting personnel who are in real-time contact with children (e.g. moderators);

IV. Terms of service – the conditions governing how the service may be used, what the minimum registration age is, what is inappropriate use, what happens when terms are breached;

V. Educational materials – links to materials allowing parents, teachers, and children to acquire knowledge and practical skills (e.g. on the use of technological tools).

In an Annex to the SSNP, special attention is paid to Application Programming Interfaces (APIs) – i.e. third-party applications which users can integrate into their SNS profile or account to add functionalities – that can raise particular safety issues. Depending on whether or not there is a relationship between
the SNS provider and the API developer, providers may be expected to take responsibility for the service in light of the SSNP when there is a direct relationship or – if no relationship exists – to at least provide advice to users on how to remove links to APIs that breach their safety policies.

**Compliance**

In order to monitor the implementation of the SSNP, a self-declaration form has been developed for SNS providers to report on the status of their safety measures to the European Commission; the non-confidential information in these self-declarations is published. These declarations are used as input for independent implementation assessments. To date, there have been two assessment reports. In 2010, it was found that the majority of a total of 25 service providers score well on compliance, and none of them score poorly. Overall, Principles 1 (awareness), 3 (user empowerment) and 6 (privacy) are well implemented; however, with regard to principles 2 (age appropriateness) and 4 (reporting mechanisms), the majority of the service providers are only partially compliant (Staksrud and Lobe 2010). In May 2011, fourteen SNS services were assessed, four of which were labelled “unsatisfactory”. In these cases, Principles 1 (awareness) and 4 (reporting mechanisms) proved to be the best implemented principles by the SNS providers. Principle 3 (empowerment) was the most poorly implemented principle, particularly because with most SNS services, minors could be contacted by non-friends and their profiles could be accessed by those outside their accepted contact list. None of the SNS providers scored “very satisfactory” on either of the principles. Moreover, the 2011 assessment separately focused on nine other SNS platforms, including photo/video sharing platforms, virtual worlds, blogging and gaming platforms. None of these services were assessed “unsatisfactory” on the tested principles; two services scored “very satisfactory” on each of the tested principles (Donoso 2011). In 2012, a midterm review of the implementation of the principles showed that despite progress in some areas important steps still need to be taken, e.g., with respect to age-appropriate privacy settings and content classification.

**Effectiveness**

The assessment reports do not necessarily reveal how effective the SSNP have been since their adoption. However, given the fact that there are still – sometimes major – gaps in compliance, we can conclude that they have not yet had the overall intended effect. The fact that the principles are a relatively recent initiative is also a factor. Moreover, based on the results of the compliance reports, the effectiveness of each of the principles seems to vary greatly,
both in terms of implementation and assessment period. All in all, this means that there is still work to be done with regard to the implementation of the principles within these SNS services. In addition, it would be advisable to test whether the measures that have been implemented actually contribute to the objectives of the principles, e.g. by performing user studies.

Although research on effectiveness is lacking, certain factors may have contributed to at least a partly successful implementation of the principles:

- Sharing of expertise and experience by multiple stakeholders;
- Commitment of stakeholders;
- Societal relevance of child safety;
- Social-economic relevance of online social networking;
- Assessment of safety practices.

In the absence of formal evaluation of the impact of SSNP, continuous monitoring of safety practices remains important. Moreover, more information on the (cost-)effectiveness of measures and user experiences is needed in order to fine-tune the implementation of the principles.

Framework for Safer Mobile Use

A public consultation on child safety and mobile phone services in 2006 highlighted a number of alarming developments in this field:

There is a wide consensus that, along with all the benefits that mobile phones bring to young people, some risks exist. Main risks identified confirm the evaluation made in the consultation report: harassment and bullying, grooming and sexual discussions, mis-contracting with minors, access to chargeable content, fraud and spam, high expenses, exposure and access to illegal/harmful/adult content, pornography and violence and risks concerning children’s privacy, in particular due to the inappropriate use of camera phones and location services. (European Commission 2006: 3).

Although there was a consensus that a shared responsibility of parents/carers, industry and governments exists, self- or co-regulation was seen as the most appropriate regulatory strategy to address these issues. Existing self- and co-regulation in some countries was generally perceived as “effective and well-balanced” (European Commission 2006: 7).
Commitment

Consequently, in 2007 the mobile industry – encouraged by the European Commission and in response to a public consultation – established the “European Framework for Safer Mobile Use by Younger Teenagers and Children”. The Framework was discussed by a High-Level group established by then Commissioner for Information Society and Media, Viviane Reding, which consisted of mobile operators, content providers, child-safety and consumer organisations, and regulatory authorities. The Framework is a hybrid form of self-regulation, involving both industry and Commission collaboration, the goal of which is “to ensure safer use of mobiles, including by younger teenagers and children”. Since June 2010, 83 mobile operators (96% of the total telecom market addressed by the Framework) have signed the Framework and national implementations have been carried out in 25 EU member states.¹⁷

Recommendations for measures to be implemented on a national level include:¹⁸

- Classification of commercial content – content of mobile operators themselves and third party commercial content should be classified to make it clear which mobile content was harmful or unsuitable for minors;
- Access control mechanisms – parents should be provided with effective tools to block access by children to undesirable mobile content;
- Education and awareness-raising – mobile providers should raise awareness among parents and children about the risks of mobile services and should be available for questions and complaints about these services;
- Fighting illegal content on mobile community products or the Internet – cooperation with law enforcement agencies, national authorities and organisations such as INHOPE in the battle against pornographic images of children and other illegal content that is circulated by mobile phones.

Compliance

Since their adoption, three implementation reports have been published by the European Commission.¹⁹ The most recent one, the 2010 report, notes that compliance is generally perceived as high with some operators even taking additional measures (national monitoring, transparency mechanisms, spending limits).²⁰ Nonetheless, operators are also expected by NGOs to take further action in light of new technologies, particularly the growing use of smartphones (“mini-computers”). A particular concern noted by the report is the fact that parents need support (notably, information and education) to be able to understand and address risks arising from the use of mobile devices by their children. Moreover, it is believed that operators could be
more pro-active in integrating risks identified by NGOs in their solutions or adapting them accordingly.

In 2010 the industry, represented by GSM Europe, which promotes the interests of mobile operators in Europe, held the opinion that they were successful in implementing the Framework.\(^{21}\) In Denmark, for example, the “Consumer Ombudsman’s Guidelines on Marketing Practices in Relation to Children and Young People” have been implemented, encouraging marketers to target only ethically acceptable advertising to children. Also, Danish operators agreed to set spending limits: a warning notification is sent by SMS as soon as the maximum has been reached. Although this service is meant for all users, it is particularly relevant for minors who do not always realise how much they are spending. In Latvia, mobile operators agreed to have mobile phone retailers register the age of minor users and to give parents the option to turn off the costly WAP connection on their children’s phones. In almost all European countries, companies have started to inform parents and children of the risks of mobile phone use, like sexting and bullying.\(^{22}\) In the Czech Republic, all mobile operators have implemented a tool to block websites with illegal content on the mobile network, using black lists provided by the Internet Watch Foundation. These examples do not necessarily prove that there is overall effectiveness and again further research and impact studies are required.

Despite the steps taken by companies to comply with the Framework, there is still debate on safer mobile use by children as a result of the increasing number of children in Europe who have a mobile phone at their disposal.\(^{23}\) A growing number of smartphones and handheld devices provide internet access to children. Among young people, the popularity of services such as Twitter, also popular on mobile phones, is increasing rapidly.\(^{24}\) In 2011, European Commission Vice-President Neelie Kroes indicated to the industry that she expects more. She argues in favour of more information to raise parents’ and children’s awareness of the risks as well as the possibilities of mobile Internet.\(^{25}\)

**Effectiveness**

The fact that the industry has taken steps in line with the Framework does not automatically imply that these measures are invariably effective. The 2010 implementation report shows a diversity of initiatives developed by mobile operators; however, the assessments did not actually measure whether children are now better protected or encounter fewer risks. Moreover, in some instances self-regulation proved insufficient. This was apparent, for example, when parents and children in the Netherlands experienced problems with SMS services. In 2007, the Dutch organisation *Mijn Kind Online* (My Child Online) reported complaints from parents about misleading SMS services. These ser-
services, offered in advertisements on websites for children and in commercials on TV networks for children and young people such as MTV, suggested that a ringtone could be downloaded for free. But instead of getting a free ringtone, users who gave their mobile number took out a paid subscription for a mobile service.

As early as 2005, a Dutch code of conduct had been drawn up, which required transparency from providers of SMS services. However, the problems being reported by parents made it clear that this code was in need of updating: the commercial conditions of the SMS services were unclear. The telecom providers, mobile network operators and SMS content providers in the Netherlands jointly drew up a new code of conduct for the provision of mobile services. Agreements were made on subscription confirmations and ways of advertising for mobile Internet services. A filter came into being: smsdienstenfilter.nl, a site where parents could block their children’s mobile number for specific services.

Stakeholders including the organisation Mijn Kind Online were consulted, but initially the industry did not adopt the key proposals to make commercial services more transparent. This was not without consequences. In January 2010 it was found that 25 percent of 12 to 18 year-olds had at some point in time subscribed for an SMS service unintentionally. For children between 8 and 12 years old with a mobile phone, this was 10 percent (Duimel 2010). In July 2010, content provider Celldorado was fined more than one million euros by the Consumentenautoriteit, a supervisory body, for deception.

Subsequently, the code of conduct was adapted once again, but this was not enough for the government – new legislation was adopted in parliament. Under the new Act, operators can refuse to deduct money from users’ bank accounts for providers who do not comply with the code of conduct. Furthermore, disputed payments for SMS services by consumers can be suspended.

Overall, a number of success factors can be identified:

- A large number of operators (96% of the EU market) are involved in the implementation of the Framework;
- National implementation of the principles result in a diversity of good practices;
- Close collaboration between the stakeholders;
- Monitoring and assessment of practices (although methodology is unclear and GSMA Europe, representing the mobile operators, is not independent);

However, ongoing monitoring and evaluation remain essential to keep up with new technological developments and trends in youths’ mobile media usage, and to ensure adequate measures and commitment by industry.
Where Do We Go From Here?

What could enable the “European Framework for Safer Mobile Use by Younger Teenagers and Children” to be more successful? What is required to make sure that minors do not see harmful or unsuitable content on their mobile phone, provide parents with effective instruments to keep their children away from undesirable mobile content, and prevent mobile phone bullying by children, e.g. by filming each other and spreading these images through mobile internet? Parents hold primary responsibility for their children’s good behaviour in using mobile phones. However, it is very difficult for parents to supervise what children do with their mobile phone and what they can see via the mobile internet. Parents need support. Through retailers, the industry can reach parents and children and give them information, besides offering tools to classify or exclude content. Good practice by retailers and by the industry could incentivise parents to purchase mobile phone products and therefore good safety practices could make good business sense. Governments, too, have a responsibility, in providing information to pupils through the educational/schooling system.

Conclusion

Increasing internet safety for children requires a joint effort on the part of the EC, national governments, the industry, teachers, parents and, last but not least, children themselves (De Haan 2009). This chapter has discussed the role of the industry and focused on how social networking sites, mobile phone operators and game content providers contribute to children’s online safety through self-regulation. These three case studies represent only a snapshot of the selected self-regulatory practices in Europe. For each case study we discussed the regulatory roles and responsibilities, and mapped central processes (formation, membership, rulemaking, monitoring, enforcement, sanction and self-evaluation) against industry needs and priorities within policy areas (cf. Cave, et al. 2008).

Due to rapid changes in the ICT sector and the emergence of new regulatory concerns (e.g. harmful content, cyber bullying, inappropriate online sexual solicitation, and illegal, risky or anti-social behaviour), the regulatory playing field in the EU continues to evolve dynamically. The EU and national governments consult with the ICT sector to determine priorities for new strategies. For both social networking sites and mobile phone operators, EU guidelines have been the starting point for their self-regulatory endeavours. In this context, PEGI is an exception, since there are no principles, guidelines or a framework from the EU or governments underlying this initiative. From the beginning, the EU provided moral support to the PEGI initiative, but the process leading to its establishment was the work of the games industry in cooperation with rating experts.
Governments can be involved in practices of the industry, giving rise to a combination of self-regulation and statutory regulation (co-regulation). Cave, et al. (2008) describe the degree of government involvement as a continuum from no involvement to the strongest intervention and draw the analogy with the Beaufort scale of wind strengths, where the strongest wind levels (9-11) represent degrees of co-regulation (i.e. government legislative force behind the regulatory forum). On this scale PEGI scores 7, a form of self-regulation close to co-regulation. We estimate that the wind force of the self-regulatory systems of SNS providers and the mobile telephone industry to be of similar strength.

Self-regulation is relevant and often preferred to other approaches, because the technological landscape is constantly changing, giving rise to an ever increasing diversity of online risks for children. Negotiations between all EU Member States would be too time consuming a process to bring formal legislation up to speed with EU and international internet developments. The flexibility of self-regulation and the know-how within the ICT sector can respond more quickly when it comes to creating opportunities for improving online safety conditions for children.

The examples discussed in this chapter show that industry is capable of securing the commitment of its leading players. The Safer Social Networking Principles for the EU were adopted by 20 major social networking service providers (SNS providers) in Europe. The mobile telephone industry states that they have been able to give effect to the European Framework for Safer Mobile Use by Younger Teenagers and Children and the PEGI criteria for the classification of games (age classifications and content descriptors) have been uniformly introduced throughout Europe and adopted by over 800 publishers of international games for a total of more than 18,000 games.

Signing up to self-regulatory principles does not necessarily mean that they are always fully implemented. Independent implementation assessments of SNS providers indicate that there are still – sometimes major – gaps in compliance. In particular, in relation to user empowerment through tools and technology principles, age appropriateness and reporting mechanisms, a majority of services are only partially compliant. Initially, the code of conduct among telecom providers and SMS content providers was not satisfactory: SMS services were not sufficiently transparent. The large number of victims of opaque SMS services in the Netherlands example showed that the industry’s self-regulation turned out to be ineffective. It was only after legislation was introduced that more adequate protection was achieved. The legislation was an incentive for the industry to become more active. Contrary to these findings, compliance within PEGI compared to the SNS sector and the mobile phone sector turned out to be very high.

The ultimate test for the success of self-regulation is the improvement of online safety among children. Many children continue to encounter age-
inappropriate content or conduct, necessitating urgent improvement of various kinds of protection strategies. However, hardly any research is available to measure this impact of self-regulatory systems. Online safety is influenced by many factors and it is difficult to distinguish between the impact of self-regulation and, for example, the influence of parents or teachers. This requires longitudinal studies and some patience before results can be expected. Yet, this kind of impact assessment is strongly needed to draw conclusions on the overall effectiveness of self-regulation. Transparent performance information on both compliance and safety impact is needed.

High compliance in the PEGI system and lower compliance in the other two systems raise an interesting question as to whether conditions for successful self-regulation can be formulated. Compliance with the PEGI system is effectively organised by the support of the three major console producers who demand that game producers add content labels and an age classification to their games. Furthermore, an independent complaints commission and a scientific advisory board contribute to PEGI’s authority. The possibility of financial sanctions reduces the attractiveness of non-compliance. Such strong regulatory instruments are lacking in the other two cases. “Showing its teeth” to a member by means of some kind of sanction is considered to be a test of the effectiveness of self-regulation (Cave, et al. 2008). Besides financial sanctions (possible within PEGI), other sanctions may be possible, such as withdrawal of membership (and loss of prestige) and censure for non-compliance (not possible within PEGI). Without the opportunity to impose sanctions, the industry may favour profit over safety, as the case of SMS services in the Netherlands has shown. If self-regulation targets other goals such as providing safety information, successful implementation is more likely. The industry is better positioned than government for providing such information to consumers. Yet, as Cave, et al. (2008) note, there is no “magic bullet” in internet regulation, or in terms of successful formulas for self-regulation.

Notes
1. www.pegi.info
2. www.isfe.eu/objects/age-rating
3. Following a dramatic shooting incident in Erfurt in April 2002, Germany opted for its own game rating system.
4. www.isfe.eu/objects/age-rating
5. www.isfe.eu/objects/age-rating
7. www.pegionline.eu
8. At the end of 2011, PEGI Online underwent a few changes, making it possible for publishers to be compliant on a game by game basis.
9. For a list of the 20 signatories, see <http://ec.europa.eu/information_society/activities/social_networking/eu_action/selfreg/index_en.htm>. Signatories involve both relevant international (like Facebook, MSN and Youtube) and local SNS providers, which implies a broad coverage of SN services used by youths.

10. See Livingstone et al., 2011, for most recent data on online social networking risks.

11. Information provided to users should be presented “in a prominent, accessible, easy-to-understand and practical format” (EC, 2009: 6).

12. E.g., even if children have a closed SNS profile, APIs may open up communication channels with people they do not know have not friended.

13. Additionally, trends in safety practices and user (risk) behaviour as well as the effectiveness of the SSNP are discussed with other stakeholders every eighteen months.

14. Principles 5 and 7 were not tested due to ethical considerations.

15. Again Principles 5 and 7 were not tested due to ethical considerations.


24. In the Netherlands, the police have their hands full with ‘dreigtweets’ (threats on Twitter) by young people threatening, for example, to blow up their school, which after police questioning turns out to be “only a joke”.


26. Besides Mijn Kind Online, the consumers’ organisation Consumentenbond and the National Ombudsman advised the industry, united in the foundation Stichting SMS-Gedragscode, see: www.smsgedragscode.nl.


28. In the Netherlands, a product especially for children is offered by telecom provider KPN: Hi Young (www.hiyoung.nl). Here, all commercial SMS services (such as paid ringtone subscriptions) are blocked automatically. If the credit has run out, the child can send a free emergency SMS to his/her parents.

References


129
Part II
Policy Players
Chapter 7

The Changing Role of the Media Regulator

Brian O’Neill

Coinciding with rapid change in the media environment and the blurring distinctions between traditional media and online services over the course of the last decade, a steady transformation has also taken place in the regulatory arrangements that underpin the communications sector. In the move towards a converged media environment in which hitherto distinct sectors of broadcasting, telecommunications and the internet operate more or less seamlessly across diverse platforms, the changing face of governmental regulatory authority within the policy landscape – and the role of the media regulator – is one of the most distinctive points of contrast between old and new media worlds.

Since the early 1990s, European Union policy has supported a policy of market competition and technological neutrality with regard to the different services that have traditionally been subject to separate regulatory regimes (Ofcom 2006). A move towards ‘better regulation’ in the technological sphere (Reding 2005) has been accompanied by a shift towards, in the first instance, models of ‘converged’ regulation whereby one regulatory authority assumes responsibility for both content and transmission services across different sectors, and secondly, towards greater use of self-regulation by industry on the basis that it is best placed to respond to the fast-moving technology environment. On the face of it then, there would appear to be, at least within the European context, a declining role and less need for public regulation or regulatory bodies (see chapters 4 and 6, this volume).

Certain public policy objectives however – e.g. the protection of minors, the prohibition of incitement to hatred – as well as fundamental values of freedom of information and cultural diversity are of such importance that public regulatory oversight of the audiovisual sector remains a priority. The availability of audiovisual content across a spectrum of traditional and new media platforms, from television through to set-top boxes delivering video, games consoles, tablets, laptops, mobile devices and smart phones, fundamentally transforms the traditional ‘command and control’ relationship that regulators
once had with the media industry. In its place, national regulatory agencies (NRAs) articulate values that underpin regulation of services, implement rules that protect those values, and foster good practice through oversight of co- and self-regulatory schemes.

This chapter, therefore, looks at what this changing role means for the traditional regulatory function of monitoring compliance with community standards, what may be called its ‘moral watchdog’ role (Ong 2010) with particular reference to protecting children in the media environment. National regulatory agencies in the main are understood to be those bodies charged with responsibility for implementing the aims of European audiovisual media policy (INDIREG 2011). Typically, such bodies do not have a specific remit for the internet or for internet safety. Yet, in implementing policy on protection of minors, more and more regulators must also deal with questions of access to online content. In this chapter, therefore, examples are chosen not just from the traditional media environment, but from regulatory oversight of companies offering internet services. Three examples are put forward to illustrate regulation in transition: (1) content regulation for new media as it applies in the German Youth Protection System – the closest to traditional content regulation as such; (2) regulatory oversight of data privacy, with particular reference to the Irish situation; and finally, (3) promotion of media literacy as practiced by the UK regulator, Ofcom. Finally, considering the role of the media regulator as a policy actor, the chapter examines the scope for regulators to contribute to the policy making process itself in generating or setting policy goals and standards.

The Function of Regulation

Under European Union law, media regulation is the autonomous responsibility of individual Member States. Through directives, the European Union aims to harmonise the law across EU Member States in sectors such as the audiovisual and media sector, setting out objectives to be achieved but not telling Member States how to go about achieving these objectives. Interpretation and implementation of directives, therefore, falls to national bodies and media regulators of various kinds. As a result, there is wide variation across Europe both in terms of the density of media regulation within countries and the kinds of regulatory agencies used to implement policy.

Regulatory bodies occupy a central but changing role within the wider process of governance and rule-making within society. The OECD (1994) defines regulation as ‘... a set of incentives established either by the legislature, government or public administration that mandates or prohibits actions of citizens and enterprises’ (p.8) and the regulator as the body that has statutory recognition to undertake functions such as:
• The formulation of goals, the making of rules, [and/or] the setting of standards;
• Monitoring, gathering information, scrutiny, inspection, audit and evaluation;
• Enforcement, modifying behaviour, applying rewards and sanctions.¹

Public regulation typically oversees both formulation of legislative and regulatory rules and oversees their implementation. Regulatory bodies are likely, but not necessarily, to be in the public sector and to be nominated by government and supported by public funding. Crucially, a regulatory body is one that is said to have statutory backing by virtue of being recognized as a regulatory authority in legislation. In keeping with European principles of better regulation and government (Council of European Ministers 2001; Reding 2005), regulatory bodies are also defined as being independent organisations, separate from any other body with the capacity, personnel and resources for autonomous decision-making and with an expectation of consistency and continuity over time. The advantages of direct or public regulation may be said to derive from its authority as a democratically accountable process, appointed to represent the public interest and with the ability to impose sanctions in the name of the state. Against public regulation, it is often said that the process of developing regulatory rules by public bodies is too slow, expensive and insufficiently equipped to deal with the complexity of change in a fast-moving technological environment (Palzer and Scheuer 2003).

Traditionally, a ‘command and control’ approach to the economic management of the broadcasting sector was deemed the most appropriate means of safeguarding national interests – whether in technical areas such as spectrum management, or in relation to content, for instance in relation to protection of intellectual property rights. A central function of the regulator to date has been to ensure competition in the market place by legislating against monopolies and defining rules in legislation for market participation. With the blurring of boundaries between the underlying technologies of communication, a key driver towards more dynamic and effective management of the burgeoning market for new content applications has been the adoption of market-based mechanisms, minimizing regulatory involvement in acting as a gatekeeper to the market and allowing operators and service providers to determine the optimal uses of spectrum. From an economic point of view, distinct rules governing markets for wireless or wired networks no longer make sense once the technologies delivering the content become fundamentally the same.

Yet in addition to their economic role, regulators have important social functions in promoting policy goals or outcomes that are not otherwise guaranteed by the market. Thus, regulators in addition to ensuring effective functioning of
the market also pursue policy goals such as securing universal service obligations from market providers to ensure the widest accessibility of communication services, and through licensing conditions to ensure audiences are protected against exposure to harmful or offensive content, that there is sufficient diversity and quality of programming content, and that there is an appropriate distinction between advertising and editorial content (Ofcom 2006).

How such societal goals can be best promoted beyond the ‘command and control’ model remains a topic of much debate. In countries such as the United Kingdom, Ofcom acts as a converged independent regulator for the communications sector, regulating the TV and radio sectors, fixed line telecoms, mobiles, postal services, plus the airwaves over which wireless devices operate. A number of other countries, including Italy and Finland, have also moved decisively towards this ‘converged regulator’ model. Others, such as Ireland, have retained separate regulatory arrangements for discrete sectors with a consequent dispersal of responsibilities across a number of different agencies. Thus, in the context of highly differentiated arrangements for public intervention in the communications market place across Europe, with varying amounts of legislation regarding audiovisual content, how does the state act to implement public policy goals such as internet safety and protection of minors online?

Towards ‘Better Regulation’

Two broad movements may be identified as having significantly repositioned the state as a regulatory actor in the communications policy sphere. Firstly, there is a move towards distancing government from direct regulatory involvement through the establishment of independent regulatory authorities (IRAs) as the designated regulatory authority acting on behalf of the state. Secondly, there is at the same time a decisive transfer of regulatory responsibility for a host of new communications and online services to a variety of self- and co-regulatory schemes within which industry players themselves play a direct role in defining appropriate codes of conduct. Both may be said to be part of a broader movement towards “better regulation” in the European sphere (Commission of the European Communities 2001; Council of European Ministers 2001).

The rise of IRAs was a relatively novel feature of the European landscape, which traditionally had relied upon direct governmental regulation of the market. IRAs were thus set up as separate regulatory actors in sectors as diverse as energy, financial services and communications, acting on behalf of the state but defined by independence and constituting a third force between government and the sectors regulated (Thatcher 2005). The European Commission, for its part, recognises, what it terms, independent regulatory authorities (IRAs), principally the national media regulator or relevant government authority, as the
agency responsible for ensuring the implementation, oversight, and enforcement of European and national legislation. As such, the regulator is assumed to be the agency responsible for transposing European directives on broadcasting and on-demand services into national law, including protection of minors, alongside any additional responsibilities or other regulatory functions in areas such as publishing, transmission, or distribution, defined at a national level.

Delegating authority to industry players through co- and self-regulatory schemes, facilitated by IRAs, is another feature of the withdrawal from direct state or government control of the communications sector. The European Commission through its first Safer Internet Action Plan (European Commission 1999) strongly encouraged industry and Internet Service Providers (ISPs) to develop self-regulatory measures, based on codes of conduct and cooperation between industry parties, to deal with rising public concern about the proliferation of illegal and harmful content on the internet. Thus, as described in chapters 4 and 6, a range of regulatory arrangements best described as ‘regulated’ self-regulation or co-regulation, have emerged in the communications sector (Schulz and Held 2004), to achieve public policy goals with legal support from the state but leaving significant discretionary power to non-state bodies. The focus in this chapter is on the state end of this relationship, and the means by which state agencies achieve public policy goals.

Protecting Children – A Legacy of Concern

The protection of children against harmful media influence is a public policy theme with a long history (Wartella and Reeves 1985; Oswell 2008; Livingstone 2009). Drawing on a legacy of concern about the impact of harmful media content on children, from the early days of radio to contemporary debates about harmful content online, regulation to protect minors pursues a public interest objective that children should be raised in a protected environment, free from the distorting influences of the adult world (Valkenburg 2004). Broadcast television acts as the principal paradigm for regulation to protect minors (Sparks 2009), on the basis that decisive regulatory intervention is required to prevent young people’s access to harmful content such as violent or adult content in primetime programming. Concerns such as the amount of time children spend with media, about violence and sexuality in the media, unscrupulous advertising aimed at children, or the lack of educational or age-appropriate content are all topics that regulators have dealt with (Wartella and Robb 2011).

Despite a long history of debate and research on its perceived negative impact on children, television was in fact some 30 years in existence before any formal regulation was introduced (Trotta 2001). In the United States, the Federal Communications Commission (FCC) retains the right to prohibit inde-
cent material during times of the day when children are likely to be viewing, an approach upheld in a Supreme Court challenge (*FCC v. Pacifica Foundation* 1978), which found that protecting children was a compelling ground for government intervention (Kunkel & Wilcox 2001: 594). In 1996, proposals for V-chip technology, enabling filtering of sensitive, violent or potentially harmful content, were also adopted by the network television industry (Kunkel and Wilcox 2001).

European directives – the Television Without Frontiers (TWF) Directive (1989), later the Audiovisual Media Services (AVMS) Directive (2007, 2010) – likewise include key provisions for protection of minors. These include restrictions on advertising in such a way that commercial communication must not cause moral or physical detriment to minors, must not exploit their inexperience or incredulity, exploit the trust minors place in adults, or unreasonably show minors in dangerous situations (Council of the European Communities 1989: Article 16). Article 22 of TWF introduced the framework, now operable in all European Member States, whereby media regulators must distinguish between programme content that might

a) *seriously impair* children’s development (e.g. programmes that involve pornography or gratuitous violence) – and which is banned on terrestrial television, or

b) *likely to impair* children’s development – and which is permitted only be transmitted at a time when minors won’t hear or see such broadcasts (the ‘watershed’) or when preceded by an appropriate visual or acoustic warning

(Harrison and Woods 2007)

The distinction between the two is a matter for interpretation by regulatory bodies with a variety of solutions as a result in different European countries, variously relying on rules excluding pornographic or gratuitously violent content, programme labelling systems that classify content and indicate its suitability for audiences of different ages, use of the watershed, and regulations regarding advertising to children (Arnoldi 2003). As such, while safeguarding freedom of expression and a diversity of programming content, the regulator must ensure that through the use of a range of tools including conditional public funding supports, licensing, and programming standards and guidelines that the television environment, for one, remains amenable to public policy intervention or centralised control (Thornburgh and Lin 2002; Ianotta 2011).

The Audiovisual Media Services (AVMS) Directive (2007) introduced a ‘graduated’ approach according to whether content is aired on linear TV services or via non-linear, on-demand services, and as such extended traditional concepts of protection against harmful content from the world of broadcast media into
a new media environment that includes streaming, downloading and other forms of online delivery.

Its principal provisions (summarised in Table 1) allow forms of ‘adult’ content, normally shown on linear television after the watershed or in encrypted form, without restriction through on-demand, online services. More harmful content, including pornography or material containing gratuitous violence which is banned on television and comes under the remit of traditional media content regulation, is allowed in an online form subject to restrictions and controls (encryption, age verification etc.) to ensure that minors will not be able to access it (2007/65/EC, 2007: Article 3). Co-regulatory regimes that are ‘broadly accepted by the main stakeholders and provide for effective enforcement’ are recommended. So too, parental responsibility, supported by filters and rating systems to guide parental discretion, is highlighted as is the need for promotion of media literacy and education of viewers.

Table 1. Overview of Graduated Regulation

<table>
<thead>
<tr>
<th>Linear (TV) services</th>
<th>Non-linear (on-demand) services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content which might seriously impair minors must ...</td>
<td>... not be included in any programme (total ban) Article 27(1)</td>
</tr>
<tr>
<td>Content which is likely to impair minors must ...</td>
<td>... only be made available in such a way that ensures that minors will not normally hear or see such on-demand audio-visual media services Article 12</td>
</tr>
<tr>
<td>... be ensured, by selecting the time of the broadcast or by any technical measure (e.g. encryption), that minors in the area of transmission will not normally hear or see such broadcasts. Article 27(2), (3)</td>
<td>No restrictions</td>
</tr>
</tbody>
</table>

Source: European Commission Audiovisual Media Policies.

It is a matter of some debate in the literature just how much the AVMS Directive reconfigures the role of the media regulator. While on the face of it, it appears to place the regulator at the heart of a regime with extensive powers over new media distribution channels, the reality of the graduated approach suggests that this extension is perhaps more symbolic than real, regulating what is already regulated and adding little to the content rules that are already in existence (Valcke and Stevens 2007; Lievens 2010). The Directive, for instance, does not grant regulators any extra responsibility or power to regulate content in the new media environment that they did not previously possess. In practice, in many countries, online services fall outside the remit of the main media regulator except for ancillary functions such as the promotion of media literacy (see below). Except where it is a fully converged regulator (as in the case of
BRIAN O’NEILL

Ofcom), frequently different state agencies, sometimes overlapping, have responsibility for discrete areas of policy including compliance with content rules, data protection or technical licensing in the case of wireless communications. Content regulation, therefore, effectively remains technology- and medium-specific, with broadcasting operating under one regime and internet services under a variety of other self- and co-regulatory schemes. In the traditional media environment of radio, television or cinema, there are well-established systems of regulation and public oversight that comprise national regimes of licensing, content classification, rules governing scheduling of content and forums for public redress through relevant industry councils and complaints commissions and so on. Within the digital environment, policy objectives such as protecting audiences against exposure to harmful or offensive content are devolved to the industry and to users with minimal provision for oversight through regulation.

Recognising the increasingly blurred boundaries between such old and new media in a fully converged world, the European Commission’s Green Paper (2013) calls attention to the suitability of current regulatory instruments and to the distortions that arise where there are different regulatory provisions for different market actors providing audiovisual content. Anomalies arise therefore when the same content is available on different screens, posing different challenges for age verification, for controlled access, labelling or complaint reporting in the case of harmful or even illegal content.

Accordingly, traditional approaches to content regulation are implicitly weakened through convergence and – with protection of minors specifically in mind – no longer act as the primary means of guarding against harmful media influence. To illustrate further the challenges posed in a fast transitioning regulatory framework, the following section looks at three examples of media regulation that address the new media environment from the contrasting perspectives of content regulation, privacy protection and media literacy promotion.

The Regulator in Transition: Three Examples

*The German Kommission für Jugendmedienschutz (KJM)*

Germany’s youth protection system for the media comprises a complex and strict set of rules governing audiovisual, broadcast, gaming and online content. As a federal republic, Germany’s Kommission für Jugendmedienschutz (KJM) (Commission for the Protection of Minors in the Media) acts as a central authority for Germany’s sixteen Länder to set standards for the rating of content and monitoring of compliance under Germany’s Interstate Treaty on the Protection of Human Dignity and the Protection of Minors in Broadcasting. As the primary legislative framework to implement AVMSD requirements, the Interstate
THE CHANGING ROLE OF THE MEDIA REGULATOR

Treaty specifies rules for service providers, detailing content that is illegal and forbidden on all services (e.g. child pornography, content glorifying violence etc.), content that may be available on telemedia or on-demand services but not on broadcast television (adult pornography, for instance), as well as the appropriate protection mechanisms required of service providers to ensure that content not suitable for certain age groups is effectively made inaccessible to young persons through, for example, age-verification mechanisms or access-blocking software (Schulz, Held et al. 2008).

Some features of the organization and tasks of the KJM may be seen as typical of traditional media content regulation. It is the central media regulator that analyses and assesses whether audiovisual content breaches the provisions of the Interstate Treaty and proposes appropriate measures that are then implemented by the state media authorities. It specifies transmission times for certain types of content, analyses and approves encryption and blocking systems and certifies technical systems for the protection of minors. In addition, the KJM responds to and files applications for listing problematic internet content in an index of harmful media maintained by the Federal Department for Media Harmful to Young Persons (BPjM).

KJM exhibits a number of characteristics that are unique to the German system. In the federal system, individual state media authorities are responsible for monitoring and regulating within their area of jurisdiction. KJM, in this instance, acts as a central regulatory authority to ensure consistency across different states and therefore acts on behalf of the relevant media authority within each state or German Land. KJM also operates within a system of ‘regulated self-regulation’ (Schulz and Held 2001) in which broadcasters and telemedia service providers are permitted to operate without state interference as long as they act in accordance with approved and certified self-regulatory bodies acting for distinct parts of the media industry. The KJM, in this instance, is responsible for certifying those bodies – the Voluntary Self-Regulation of Television (Freiwillige Selbstkontrolle Fernsehen, FSF) and the Voluntary Self-Regulation of Multimedia Service Providers (Freiwillige Selbstkontrolle Multimedia-Diensteanbieter, FSM). Drawing on notions of self- and co-regulation more familiar in Anglo-American approaches, ‘regulated self-regulation’ was specifically developed within the German constitutional framework to evolve a system that moved away from hierarchical control to a more arms-length approach based on ‘instruments the state can apply to regulate a self-regulatory process’ (Schulz and Held 2001: 15).

While voluntary self-regulatory bodies such as FSF and FSM are responsible for developing codes of conduct and ensuring their members comply with guidelines for the protection of minors, the KJM acts in the public interest and is the public face for matters impacting on children in commercial and telemedia services. Its central office handles complaints and requests from media users and monitors broadcasts and telemedia services. It also contributes to policy on
problematic aspects of content for young people through expert assessments, contributions to judicial processes, media relations on areas of children and media and evaluates technical measures for the protection of minors in telemedia and broadcasting services. Its reach also extends to the internet through its auxiliary agency jugendschutz.net, set up in 1997 by the state media authorities to deal with problematic online content and has the function of both monitoring the internet and responding to complaints.

A core feature of the German system implemented in the 2003 Interstate Treaty is the extension of responsibility to non-state actors for protection of minors under licence from KJM, the central regulatory authority. A review of its rules in 2010 proposed ambitiously to extend the activity of self-regulatory bodies in age-rating of content to the internet. The proposed amendment outlined a graduated approach whereby content providers could choose to: (1) rate their content according to their own standards, (2) rate their content using the rating standards of a recognized self-control organization, (3) charge a self-regulatory organization with age rating, or (4) have a government authority approve the age rating established by a self-regulatory organization (OsborneClarke.de 2011). This approach proved controversial and was rejected at state level. Accordingly, the legal regulations from 2003 continue to apply while new proposals are sought for consistent and transparent standards for content provided online. What is interesting in the failed amendment, however, was the proposal to allow media operators and service providers a high degree of autonomy to operate against the background of a strong statutory framework (the Interstate Treaty), leaving the regulator considerable scope for supervision, rather than detailed implementation, and policy development.

Data Privacy Protection: The Experience of Ireland

A different form of regulation is involved in the area of privacy and the protection of personal data, a topic that has become increasingly central to youth protection in the online environment. Concerns about data privacy protection arise with ubiquitous use of computerised data processing and storage which, combined with internet technologies, creates vast pools of data and complex international data networks that expose personal data to wide commercial exploitation and/or unlawful access. Developing and implementing laws to strengthen privacy is a priority for many countries and typically encompasses measures to protect individuals against abuse of their personal information as well as granting them the right of access to their own data in order to check its accuracy and appropriateness (OECD 2002).

As in other areas of media and telecommunications regulation, the sovereignty of each country and the right to regulate its own sector is widely recognised (for instance by the International Telecommunications Convention
THE CHANGING ROLE OF THE MEDIA REGULATOR

of 1973). Wide international recognition of the right to privacy is, however, supported under the European Convention of Human Rights (1950), the EU Charter of Fundamental Rights (2000) which under the Treaty of Lisbon (2009) acquires full legal effect and the International Covenant on Civil and Political Rights (United Nations 1966). The OECD’s Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) was the first international statement of core information privacy principles and has widely influenced the development of national legislation and codes. Yet, the explosion of new online services and harvesting of personal data for a host of purposes unforeseen at the outset of international agreements has greatly increased the importance of data protection regimes and the role of Data Protection or Information Commissioners within individual Member States.

The principal instrument within the European Union is its 1995 Directive on the protection of individuals with regard to the protection of personal data and on the free movement on such data (EU Directive 95/46/EC). This sets out the main provisions for the data subject’s right to be informed, right of access to his/her data, right to object, provisions for data security as well as questions of liability and sanctions for breaches of personal data privacy. The Directive requires Member States to establish one or more independent public or supervisory authorities (Article 28) to monitor the application of relevant data protection legislation to include powers of investigation and intervention. In addition, the Directive provides for a EU-wide Working Party, consisting of representatives of national supervisory authorities (the Article 29 Working Party) and with an independent advisory role on data protection matters.

Proposals to introduce a new Regulation to reform European data protection legislation were brought forward in 2012 and are intended to strengthen online privacy rights while seeking to boost Europe’s digital economy through a simplification of rules that would apply to companies operating in different countries (European Commission 2012). Under this proposal, intended to replace the 1995 Directive, Member States, unlike in the case of an EU Directive, do not have any level of discretion; once a Regulation has been passed, it enters in its entirety into the domestic legal system of a Member State. Specifically with regard to the role of the regulator, it is proposed that a single set of rules on data protection apply across Europe and that organisations will only need to deal with a single national data protection authority in the EU country where they have their main establishment. National data protection authorities are strengthened under the proposals. They gain the power to fine companies that violate EU data protection rules. Users may also contact the data protection authority in their own country even when their personal data is processed by a company in another country.

An illustration of the operation of such cross-national regulation was given in the case of the audit of Facebook’s privacy policies by the office of the Data
Protection Commissioner (ODPC) in Ireland in 2011. As Facebook’s European headquarters in Dublin processes data for all users outside of Canada and the US, it is subject to European privacy and consumer law. Following pressure from international privacy action groups, it fell to the Irish Data Protection Commissioner to conduct an audit of Facebook’s privacy policies and procedures for compliance with European legislation. The first report of its audit was published in December 2011 and, while its findings about Facebook’s approach to privacy policies were largely positive, some significant recommendations were made to bring Facebook’s policies fully into line with European data protection legislation. These included provisions for:

- New standards for users to convey an informed choice for how their information is used and shared on the site (including in relation to Third Party Apps);
- A more transparent Data Use Policy/Privacy Policy;
- Specific deletion periods for user data, including cookies/“social plug-ins”, search data and ad-click data;
- An enhanced ability for users to control tagging and posting on other user profiles;
- More controls on the addition to Groups by friends;
- A requirement that the introduction of new products or new uses of user data will take full account of Irish data protection law.

(Office of the Data Protection Commissioner 2012)

While the audit of Facebook was conducted under existing data protection provisions contained in the 1995 Directive and relevant Irish legislation, it does highlight the importance of cross-national regulatory oversight and the need for supervising authorities to investigate and make findings for online services that are inherently transnational in nature. In the case of European legislation, users of Facebook through agreeing with their Terms of Service have a contract with Facebook Ireland, the main headquarters for the processing of user data. The case of Europe v. Facebook was initiated as a result of complaints lodged with the Irish Data Commissioner. Under the proposals for a new Regulation, users will able to process complaints through data protection authorities in their home country while companies will only be required to deal with one authority in the country in which they are based. The balancing act in this instance is that of ensuring the best degree of protection for individual rights to privacy – supported by the appropriate regulatory bodies to enforce and monitor implementation of those rights – while reducing the complexity of different legal requirements and competing regulatory obligations for companies operating in a single, transnational market environment.
Promoting Media Literacy: The Experience of Ofcom

The promotion of media literacy is a relatively new area of activity for media regulators and one that has had considerable policy attention since its first appearance in the AVMS Directive (2007). Leading up to the new Directive, considerable political discussion was given over to the need for regulatory policy to safeguard public interests, such as cultural diversity, the right to information, media pluralism, protection of minors and consumer protection. Included in this framework was an emphasis on the role regulators should play in enhancing public understanding of transformations in the media environment and the requirement for better media literacy skills to cope with its demands (European Commission 2003). This was particularly the case in relation to youth protection matters in the audiovisual sector. While the provisions for protection of minors in the TWF were deemed to be adequate and clear for the traditional media sphere, their application to the online environment, as discussed above, raised many challenges, for which media literacy was proposed as one of the responses.

Accordingly, media literacy within the context of AVMSD is taken to refer to:

skills, knowledge and understanding that allow consumers to use media effectively and safely. Media-literate people will be able to exercise informed choices, understand the nature of content and services and take advantage of the full range of opportunities offered by new communications technologies. They will be better able to protect themselves and their families from harmful or offensive material. Therefore development of media literacy in all sections of society should be promoted and monitored. (2007/65/EC, para 37)

The principal requirement set out in the Directive is for the European Commission to report on levels of media literacy in all Member States from 2011 onwards, for which a detailed set of indicators have been developed (European Association for Viewers Interests 2009). The promotion of media literacy by all stakeholders, including regulatory authorities has received sustained emphasis in other aspects of European audiovisual policy with the European Commission in 2007 calling on regulators ‘to get more involved and to cooperate in the improvement of the various levels of media literacy’ and to ‘promote systematic research into and regular observation of and reporting on the different aspects and dimensions of media literacy’ (European Commission 2007: 8).

In the United Kingdom, the Communications Act of 2003, anticipating European developments by some years, granted Ofcom, the independent regulator for the UK communications industries, a responsibility to promote media literacy among the general public. Ofcom’s implementation of its media literacy brief provided the template for public policies elsewhere and was eagerly watched by governments in many parts of the world (Lunt and Livingstone 2012). Section 11 of the Act identifies a number of features of the electronic media
environment towards which Ofcom is required to bring about (or encourage others to bring about) a better public understanding. These include the nature and characteristics of media content, the processes by which such content is selected, how media are regulated, how users can regulate and control their media access. Following a public consultation, Ofcom put forward the ‘ability to access, analyse, evaluate and produce communications in a variety of forms’ as its operational definition of media literacy (Ofcom 2004). Its activities were subsequently focused on two key elements:

- Providing an evidence base of UK adults’ and children’s understanding and use of electronic media;

- Sharing the evidence base with a wide range of stakeholders internally and externally and support their work via research. The transposition of media literacy as a matter of regulation rather than its traditional location within education has been a novel and to some extent experimental development (Lunt and Livingstone 2012: 138). Where hitherto, media literacy debates within the field of education have tended to be polarized between protectionism against harmful media influence and empowerment of young people, its more recent manifestation has shifted the debate towards questions of digital inclusion and participation. Hence, the emphasis of Ofcom’s research into adult media literacy, for instance, has tended to address issues of competence, technical skill and access to the full range of information society services. Such questions, arguably, are more amenable to empirical research and the extensive studies of user access and participation have done much to transform media literacy from a critical/theoretical and educational discourse into one founded on evidence and driven by socio-technical indicators. That said, many of the objectives of media literacy policy remain somewhat opaque, resistant to precise measurement and sit somewhat uncomfortably within the regulator’s range of commitments. While AVMSD recommends Member States to take action to improve levels of media literacy among the general population, only a limited number of countries have formally incorporated media literacy within legislation or within the terms of reference for national regulatory authorities (EPRA 2008). In most countries of Europe, regulators argue that other provisions within their mandate, including protection of minors, ratings and classification, indirectly contribute to media literacy among the population. In addition, media literacy activity has traditionally been one in which civil society has played a leading role and, in many cases, media authorities are content to support initiatives or to work in partnership with independent groups in community education and media literacy promotion.
Conclusion

The proliferation of new services and communications opportunities in today’s media environment is accompanied by increasingly complex and diverse regulatory arrangements in which the role of the national media regulator is augmented by both extensions to its traditional remit as well as by shared and sometimes overlapping responsibilities with other regulatory agencies. Fundamentally, this does not mean there is no role for the media regulator in the new communications environment: the role of the regulator remains crucially important, if different, to traditional media regulation.

There are a number of functions that the media regulator alone is in a position to supply and which are crucial to the successful delivery of policy objectives through self-regulation. In the first case, regulators have a crucial coordinating role in the development, implementation and delivery of regulatory initiatives involving multiple stakeholders. In order to address a lack of credibility in the co-regulatory process, research produced for the European Commission recommended that regulators should play a stronger role in building the capacity of the sector, through convening a co-regulatory forum at its own offices and underpinning the process with the appropriate level of technical and administrative support (PCMLP 2004). This, it noted, would add much-needed transparency to the process, building confidence and adding weight to the operation of self-regulatory schemes.

Secondly, somewhat relatedly, regulators have a crucial role to play in accreditation or validation of self-regulatory frameworks as well in their evaluation. In practice, many of the most important self-regulatory frameworks are multi-national in nature and therefore it is often the case that the European Commission itself acts as coordinator and convenor for stakeholder and industry participation. Accreditation and validation is something that regulators are in an ideal position to contribute. Previous examples have shown how the expertise of established agencies such as the British Board of Film Classification (BBFC) or the Netherlands Institute for the Classification of Audiovisual Media (NICAM) have been essential to validation of new approaches to codes of practice and classification schemes for new media content. Independent evaluation of self-regulatory schemes is widely recognized to be essential to their success and whether the regulator is directly involved or contracts evaluation to third parties, ensuring consistency and continuity in evaluation remains massively important. Regulatory agencies are uniquely qualified to undertake auditing of self-regulatory activity, including assessment of market structure, gaps and impact on fundamental rights, ensuring transparency and effective participation.

A third area in which regulators are well placed to support regulatory schemes is through promotion and awareness-raising. Successive studies have
called attention to the lack of public awareness of self-regulation in the new media environment. Most Europeans are unaware of where to report potentially harmful content and only 13% are aware of self-regulatory ISP solutions or Hotlines (Eurobarometer 2004). Such knowledge gaps continue to be a major obstacle in the delivery of the promise of co-regulation. Given the major shift of responsibility from institutional authorities to private individuals and families (Helberger 2008), an ill-informed public both undermines the credibility and effectiveness of regulation and creates a further dimension of the digital divide. Relatively, one of the functions that AVMSD ascribes to regulatory authorities is that of the promotion of media literacy, including a statutory function to promote a better understanding of the media environment and its regulatory structure and organization.

Finally, the regulator can play a valuable role in extending reach of policy development for ever-converging media. As critics of European media policy attest, legislation and policy towards convergence has not yet reached the stage where full technological neutrality is recognized or where principles of regulation can be equally applied across all platforms. With constant development of new services and new sources of content available, for instance, the burgeoning field of user-generated content, new regulatory challenges are posed which media regulators are well-placed to address. Through regulatory forums and by virtue of their central role within the media marketplace (if not in terms of actual regulatory intervention), regulators can highlight areas of need, convene multi-stakeholder dialogue on emerging issues and supply technical and legal expertise in the search for new solutions.

As noted by Cave et al (2008), ‘governance’ rather than ‘regulation’ of the communications environment may be a better descriptor for the kinds of relationships forged between regulatory agencies and industry players. At the end of a decade of regulatory reform and development, it is clear that self-regulation enjoys high level endorsement within the European Union and is seen as broadly effective for meeting the policy goal of protection of minors in offline and online services. While the state’s involvement continues to be defined by a legal relationship, it can no longer be seen to have a monopoly on the knowledge required to manage the sector or the resources required to manage its development. Finding a happy medium between direct state management and pure self-regulation is thus the responsibility of the mediating regulatory agency, deriving its authority on the basis of its legal connection to the state and the ever-present threat of further state legislation and control as an enforcement strategy.
Notes

1. See chapter 4, this volume for further discussion on the concept of ‘regulation’, command-and-control regulation, and the state’s role as legislator, adjudicator and enforcer.


3. http://www.jkm-online.de/en (some pages in English)

4. Directive 95/46/EC on the protection of individuals with regard to the protection of personal data and on the free movement on such data. OJ L 281, 23.11.1995, p. 31.

5. The office of the Irish Data Protection Commissioner was established under data protection legislation implementing the provisions of EU Directive 95/46/EC. It is a regulator appointed by government but independent in its functions and is responsible for upholding the rights of individuals as set out in the Acts, and enforcing the obligations upon data controllers. See http://dataprotection.ie/

6. The audit was instigated by Austrian student, Max Schrems, who initiated the Europe vs Facebook campaign, which lodged 22 complaints with the data commissioner’s office. See http://europe-v-facebook.org/


9. Lunt and Livingstone (2012) note the shift in policy towards media literacy within Ofcom following the change of government in the United Kingdom in 2010, the slimming down of the media literacy unit within the organization and the less committed approach exhibited by the new government.

10. The United Kingdom (Communications Act 2003), Ireland (Broadcasting Act 2009), and the 14 regional authorities in Germany, are the main examples of regulators with a legal duty to promote media literacy.

11. See, for example, the discussion of PEGI in chapter 6, this volume.

References


Chapter 8

Industry
Towards the Socially Responsible Internet

_Industry CSR Practices Across Europe_

Bence Ságvári & Miklós Péter Máder

The topic of children’s online safety, a key driver in shaping internet regulation across Europe, has for many internet service providers (ISPs) and online content providers moved to the forefront of their corporate social responsibility (CSR) practices. Research shows that to be effective and to avoid being overly protectionist, children’s online safety requires a complex mix of multi-stranded and multi-stakeholder approaches (Livingstone and O’Neill 2010). Digital safety policy is about finding the right balance between regulatory and legislative interventions on the one hand, and awareness-raising and educational initiatives on the other. While the former rests on state and international regulation, supported by self-regulatory measures on the part of industry, responsibility for the latter – given the slow progress in integrating internet safety into the school curriculum at least in several countries across Europe (see chapter 10, this volume) – resides primarily with industry and NGO initiatives.

The aim of this chapter is to look more closely at the involvement of industry, in particular ISPs, in supporting safer internet policy in Europe and the kinds of strategies companies follow to reduce the risk and harm associated with children’s internet use. Firstly, we briefly review the industry perspective on questions of regulation of the internet and locate online safety within the main regulatory models and paradigms. We then look at corporate social responsibility practices, specifically questions of liability, trust and confidence towards ISPs. In the second part of the chapter, we discuss corporate social responsibility within the context of conceptual models of the regulatory space, illustrated by real industry examples of best practice from major European telecommunications and internet companies.
Brief Overview of the Regulatory Environment

Phases of Regulation

From an engineering perspective, the internet has always been more or less self-regulated (Tambini, et al. 2008). Direct governmental interference in the development of the internet was minimal, and the underlying technological rules and standards by which it evolved were developed largely by self-regulatory bodies such as W3C (World Wide Web Consortium) and IETF (Internet Engineering Task Force).

In terms of regulation, John Palfrey has identified four distinct phases in the development of the internet (Palfrey 2010). The first period was characterized by the idea of internet as a separate domain and up until the end of the 1990s in most countries online activities were outside the radar of the state or only very weak regulation applied. Penetration rates were very low and the social and economic impact of the internet was very far from what it is today. Comparing the genesis of the commercial internet to traditional media such as radio and television there is one major difference in terms of regulation: in most countries internet service providers do not need a government license for their operations, a fact that has had a major impact on the development of services. At the same time, its evolution was also underpinned by a dominant libertarian belief in the free and universal access to information as well as the democratizing and transparent nature of the network. It was also widely held (an argument that still exists in some forms) that the internet represented a separate world (that of cyberspace) with special qualities that made its regulation impossible, even counterproductive. During this period, the internet was relevant only to a small minority of people and clearly the risks and potential threats faced by users (including children) were minimal both in quantitative (i.e. number potential risks) and qualitative terms (seriousness of risk and harm). This has been described as the generative period of the internet (Zittrain 2008), characterised by an almost completely undisturbed period of development for companies and almost completely uncontrolled activities of users.

The second period, that of “access denied”, was roughly between 2000 and 2005. During this phase, governments began to think more strategically about certain online activities that needed to be blocked or heavily managed. Most restrictions were based on governments’ efforts to hide certain parts of the internet from their citizens. Many types of filtering practices were developed at this time, varying in scope and technology (i.e. DNS, IP or URL filtering techniques), and much of it developed by the industry itself. At a global level, a wide range of social, religious and political information was filtered, mostly in countries with authoritarian and semi-authoritarian regimes. In North America and Europe, the problem of child pornography became the central focus of filtering and blocking (first in the Scandinavian countries) as one of the most
evident types of harmful content. In the United States, the government also introduced regulations about what kind of content children could access in libraries and schools (Weitzner and Price 1998; McClure and Jaeger 2009).

The period roughly between 2005 and 2010 could be considered as a phase of “access controlled”, a period in which regulatory approaches became more sophisticated. During this period, the number of control points increased, e.g., registration, licensing and identity requirements to control what people/organizations do online. Questions of liability and responsibility also became increasingly important. Industry players were forced to take an active part in blocking and in some countries – for example, China – in surveillance of the internet.

Palfrey (2010) argues that we have more recently entered the latest phase of development, the period of so-called “access contested”. Online activities have become an inseparable part of the lives of hundreds of millions of people around the globe. The internet has become an essential and inescapable economic, political and social priority for governments everywhere. In this phase, companies have implemented new strategies for coping with the spread of regulation and liability. In contrast to earlier periods where regulation took the form of state-to-individual control, the focus has moved elsewhere. In general, the emphasis of government regulation is on companies, constraining what they can do directly and requiring them to regulate individuals’ behaviour. This approach, for instance, can be recognised in the European Commission’s CEO Coalition initiative, which places the onus on industry as a whole to provide better tools for a safer internet. The proposed actions affect all members in the online eco-system, from media companies (content providers) to basic service providers (ISPs), by sharing responsibility for internet safety among them. Some actions and tasks are specific to content providers (e.g., content classification), while others belong more to the domain of service providers (e.g., effective takedown of child abuse material, parental controls). Since the dominant business models of the industry themselves constantly change, the evolution of the issue of obligations and responsibilities will remain an ongoing area of policy interest into the future.

The ever growing importance of safety for children.

From self-regulation to co-regulation of ISPs

Although the technology-focused, libertarian approach to the internet remains important today, rapid consumer adoption over the last decade or so has inevitably led to calls for new forms of regulation, especially in the field of child protection. Certainly, the “hands off” policy adopted by most governments in the early years of the internet is no longer tenable. Beyond the engineering and technicist perspective, the 1990s was also a period in which self-regulation
as a solution was advocated both by the EU (and its Member States) and the industry. Subsequently, the focus has shifted to a more co-regulatory approach, requiring the more active involvement of the state (Tambini, et al. 2008).

There are many reasons behind this shift in emphasis. For one, the social, economic and political significance of the internet reached a ‘tipping point’ (e.g., the rapid growth in the number of users, the more and more ubiquitous nature of online activities such as social networking, e-commerce, etc.), when ‘pure’ self-regulation was no longer sufficient. But it was also true that experience showed that many self-regulatory models lacked effective procedures for supervision, enforcement and compliance, in many cases showing merely a declaration of goodwill rather than rigorous implementation (Tambini, et al. 2008:4). A 2011 report of the European Commission acknowledged the importance of many industry self-regulatory measures. However, it also highlighted several deficiencies such as the lack of monitoring of several initiatives or the non-mandatory nature of compliance of ISPs with codes of conduct.

It is not difficult to see that the adoption of different self-regulatory measures and compliance with various codes of conduct is a necessary but not sufficient condition for achieving real progress in terms of internet safety. Without sufficient internal monitoring within organizations and third-party verification, few of these initiatives have the chance to succeed. But it is also the case that implementation of verification schemes is highly complicated and significantly increases the costs of self-regulation. Given that this is self-regulation, these are expenses that must be borne by companies themselves, making the process even more challenging.

However, self-regulation does offer a number of obvious advantages. It provides industry with a lead role in framing the regulatory environment and grants them the initiative in the elaboration and implementation of policy. Self-regulation has also distinct advantages for society as well, given that government-initiated schemes can in many cases be too slow and overly bureaucratic, and prove inadequate in keeping pace with the fast changing technology and service environment. More recently, all the major regulatory initiatives in children’s online safety were for the most part initiated by the European Commission, and therefore are more accurately described as examples of co-regulation.

The Safer Mobile Use by Younger Teenagers and Children, for instance, was adopted by all leading mobile operators in 2007. These EU-supervised, though largely self-regulatory measures included access controls for adult content, awareness raising campaigns, classification of commercial content and fighting against illegal content on mobiles. The first self-regulatory agreement for social network companies (following the EU’s initiative) was signed in 2009. The Safer Social Networking Principles included commitments regarding awareness raising, age appropriate services, user empowerment, easy to
use reporting tools, response to notifications of illegal content or conduct and safe use of privacy settings.

In December 2011, 25 CEOs of leading ICT companies at the invitation of Vice-President Neelie Kroes joined forces and published their proposals for a safer internet for children and young people in the EU. The initiative is unique in the sense that the complete value chain of the internet industry is represented by a number of major players, including social media companies (Facebook, Google), network operators and ISPs (BT, France Telecom – Orange, Deutsche Telekom, Telefónica, Vodafone, Telenor, etc.) and hardware manufacturers (Nokia, RIM, LG). The Coalition is a cooperative voluntary intervention and it is the Commission’s expectation that new members will join and adopt the solutions developed by the founding members. All participating companies are required to draft their own roadmaps and targets on how to implement the principles. According to the plans, there will be regular self-reporting on progress both at company and group level, and the principles will also be reviewed every two years. Sanctions envisaged include exclusion from the Coalition in cases of not applying the principles.

More self-regulatory in nature is the ICT Coalition (Principles for the Safer Use of Connected Devices and Online Services by Children and Young People in the EU), formulated by another consortium of industry players. This initiative covers much similar ground to that of the CEO Coalition. It includes principles designed to raise awareness on practices that promote online safety in areas of content, parental controls, dealing with abuse/misuse, child sexual abuse content or illegal content, privacy and control, education and awareness. Positive elements of this initiative can be found in its proposals for reporting and implementation. Much of the monitoring process is based on self-reporting of the corporate members (which does not really guarantee unbiased and independent judgement), but an independent expert panel was also appointed and financed by the ICT Principles Stakeholder Group to carry out a review of the consolidated report prepared by the signatories.

The Liability Debate

Focusing more specifically on the role of ISPs in supporting a safer internet for children, ever since the development of a mass market for the internet, the question of liability for content was from the outset the main issue in assessing the role and responsibilities of ISPs. The proponents of zero-liability usually argued that providing internet connectivity to end-users is much like any common carrier communication service, such as that of the telephone. Using a simple analogy, no telephone company could be held responsible for harmful or even criminal communication over its networks (as for example, discussing the details of a murder). Although there is some truth in this argu-
ment, the internet is much more complex than simply a transmitter of human voice. The textual, audible, graphical and video formats of digital content, and the one-to-one and one-to-many nature of communication make it a unique network of interconnected computers much closer to mass media in nature.

Cohen-Almagor (2010) has compared this special role of ISPs to a large bookstore, where the owner of the bookstore could not be held responsible for the content of each and every book on sale on its shelves. However, if it turns out that some books contain illegal content (such as child pornography) or violate copyright, the owner of the store has a legal and moral responsibility and must take action to remove the questionable material from the shelves. Similar rules have been applied to the liability of ISPs. In Europe, the E-Commerce Directive of 2000 specifies the basic principles on the liability of intermediaries and introduced the ‘notice and take down’ mechanism. According to its provisions, ISPs providing hosting services are protected from liability if:

- "the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent, or
- the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information." 8

On the other hand, most ISPs and web-hosting companies have developed their own guidelines specifying prohibited content and usage. These include not just those elements that are formulated by current laws but usually they set their own terms of use as well.

**Who Pays the Ferryman? The Issue of Monitoring Content**

Both the history of internet regulation to date and our own informal interaction with industry personnel suggest that ISPs are generally resistant to the idea of fully monitoring the content going through their servers. Their opposition can be explained by the expected costs of employing professional staff to develop the methods capable of monitoring the data flow. In addition, with current technology it is not possible to perform a complete and effective monitoring of content going through the networks of ISPs.

Another risk is that if they non-voluntarily or voluntarily accept to extend their activity to include monitoring and filtering, it will be a ‘crossing the Rubicon’ moment for the industry. As mere intermediaries in content distribution they are legally protected from liability, but if they engage in any filtering of content they become liable right away. It is also worth noting that fighting against illegal content in a constantly changing technological environment is much like a game of cat and mouse. Looked at in simple terms, assuming
responsibility for content hardly, therefore, makes for a predictable business model or gives certainty for the future.

In November 2011, a ruling from the Court of Justice of the EU precluded network providers from implementing systems for large scale filtering and blocking of users’ electronic communication. The Court’s clarification made it clear that fundamental rights and the freedom of a network provider to conduct its business should be protected and disproportionate technical enforcement that infringes the rights of others is also contrary to EU law. The otherwise complicated and costly systematic analysis of all content passing through an ISP’s network undermines both consumers’ right to protection of their personal data and their right to receive and impart information.

Currently, the economically rational choice for ISPs is simply to remove any content they are notified about, and otherwise do nothing to monitor content and let end-users, the police and of course, ultimately the content providers, decide what is stored and sent over their network infrastructure (Tambini, et al. 2008: 8). Further recent developments on illegal content and copyright issues in the USA and in Europe (SOPA, PIPA, ACTA, etc.) could have consequences for the liability of ISPs which ultimately could have implications for online safety as well. However, at the time of writing the end of this process is still not resolved.

Corporate Social Responsibility in Safer Internet Use

*What ‘Lubricates’ Business: Trust*

All human action occurs in time, drawing upon a past which cannot be undone and facing a future which cannot be known (Barbalet 1996: 82)

Across the world, hundreds of millions of people use both free and paid online services everyday based on an attitude of trust. Trust in this sense is a crucial strategy for dealing with an uncertain and uncontrollable future (Sztompka 2003). We trust ISPs to provide smooth connectivity between our client computers and distant servers and not to misuse the information they gather from our browsing behaviour. We store our most trusted personal or business secrets on Google’s or in other company’s servers in forms of emails, documents, or family photos and videos. We also trust social networking sites to ensure that there will be no faults in their privacy settings: the posts I intend to share with my friends will not appear on the screen of my boss. An even more sensitive issue is that of online financial transactions. There are numerous examples of how we implicitly trust all kinds of services as well as the companies behind them for many of our daily activities. On the internet, the logic of trust is even more fundamental than that of some traditional “offline”
industries, since more and more pieces of our personal data are moving to the cloud. Of course, many people do not think about trusting a service before they start to use it. They just decide whether it is useful and/or interesting to them. However, when something goes wrong (for example, data is lost or stolen, privacy is undermined, the expected level of filtering is not working, etc.) the issue of trust becomes paramount. The reputation of a company is largely based on trust, and when trust is damaged, it easily leads to a loss of business and/or increasing costs in restoring credibility. The issue of digital confidence (especially in terms of online financial transactions) was addressed by the European Union in its Digital Agenda for Europe in 2010. In any event, this is something that most internet companies are already keenly aware of. Building and maintaining trust around their services and the company itself is a primary goal that has an unquestionable business rationale behind it. Creating a safer online environment for children by the industry could also be interpreted as a dimension of trust (O’Neill 2012). Although in this case the logic is somewhat reversed, given that the industry as a whole is more or less at the beginning of the process, so generally speaking they are in the phase of building and accumulating trust rather than unintentionally losing it. Those companies that take a leading position in providing effective tools for online safety, or are able to achieve efficient awareness raising through their communication and other initiatives could build up consumer trust first (i.e. in the groups of parents, policy makers, and of course among children themselves etc.). This could also have a definite business advantage.

Growing Importance of CSR in Safer Internet Use

In parallel with the development of self- and co-regulation, and in line with the above question of trust, industry players are increasingly considering the issue of online safety as an activity of corporate social responsibility (CSR). Clearly, companies are themselves influenced by being part of the wider social-cultural context. Employees working for internet companies are also mothers and fathers, affected directly by the problems of online security. But it is also true – as Porter and Kramer have stated – that many companies awoke to the importance of CSR only after being surprised by public responses to issues they had not previously thought were part of their business responsibilities (Porter and Kramer 2006).

Since the motivations behind CSR activities vary both between industries and countries, it is impossible to provide a universal framework for CSR in safer internet use. According to Swanson (1995), at least three main types of motivations stand out. For those companies following the utilitarian perspective, CSR is an instrument to support performance objectives (profitability, return on investment, sales numbers, etc.). In the case of ISPs and content provid-
ers, more knowledgeable and self-conscious users also mean more profits for the companies, and for that reason many of them actively engage in activities promoting digital skills. This could also have positive implications on children’s online safety since many programmes target parents and grandparents.

When the approach of negative duty dominates, companies want to demonstrate in their behaviour and communication that they conform to the stakeholder’s or to larger society’s prevailing norms and values. For example, the increased media attention on the negative aspects of internet use (especially in the case of children) and its potential threat to companies’ business interests has encouraged them to deal with this problem more systematically. In many cases, multinational telecommunication companies have integrated CSR practices on internet safety at the highest strategic level. This is then pushed down to local managers at the national level encouraging them to work on, among other things, different awareness raising campaigns, even if they had no intention of engaging in this kind of activity previously.

And finally, the positive duty approach can be defined as companies’ self-motivation to have a positive impact regardless of their purely economic or communicative objectives. This type of motivation suggests that there should be mutual dependence between companies and society, and both business decisions and social policies must follow the principle of shared values. Benefiting one at the expense of the other undermines the long-term prosperity of both. For ISPs and content providers, this shared value with society is evident in children’s safer internet use. CSR activities in this field could certainly be beneficial for society, but it is also valuable for businesses in supporting the emergence of knowledgeable and responsible future users and developing and maintaining trust towards their services and brands.

The problem of effective CSR, however, lies in the scope of these programmes. For example, a successful industry-supported initiative can contribute to the education and training of a few hundred or thousand children, but these numbers – although large in themselves – pale by comparison with the total population in need of support.

Some Evidence on the Role of ISPs

Data from EU Kids Online underlines some important issues regarding the role of ISPs in providing information and advice on safety tools and safe use of the internet across Europe (Livingstone, et al. 2011). In general, around one fifth (21.6%) of parents received some kind of information from ISPs. The picture across Europe varies widely: in Bulgaria and Spain these figures are below 10 per cent, while in Finland and Norway it is between 38 and 41 per cent. Likewise, data from other countries shows a mixed picture and in no case do ISPs act as the main source of safety information. Rather, these varying results
can be traced back to the mix of effective CSR practices of the industry and soft or hard regulatory pressure from governments.

However, there would appear to be quite a strong demand for a more intensive role on the part of ISPs in providing support for internet safety. According to EU Kids Online data, around one in four parents would like to have information and advice from such companies in the future. After the child’s school and traditional media (television, radio, newspapers, magazines), ISPs were the next preferred source of safety information.

From the perspective of children, the current role of ISPs is much less significant. Only 6 per cent of children reported receiving information from their ISPs, while 12 per cent got information from websites. But cross country differences are significant: in Austria the proportion of children receiving information from ISPs reached 14 per cent; in Spain and Italy it stayed below 2 per cent which in fact means that – according to the data – ISPs took literally no role in educating children in these countries. This does not mean that there are no industry initiatives in this field. However, their effectiveness does not reach the threshold of social visibility and measurability.

The results of the EU Kids Online survey also provide evidence on the lack of effectiveness of industry-provided reporting tools. Only a small minority of children who were upset by something they encountered/experienced online used these opportunities, since in many cases they lack child-friendly user interfaces or easy operation (Livingstone, et al. 2012).

Conceptualizing Industry Strategies

State vs. Self-regulation

In order to better understand the activities of ISPs and content providers in this area, an overview of the legal, ethical and regulatory framework is required. The industry’s field of operation is determined primarily by the regulatory environment. However, it is also shaped by other factors such as cultural-political traditions, dominant values of the society, the general conditions of civil society and, last but not least, by the advocacy skills of both government and companies. The regulatory landscape can itself be characterised by on the one hand, legislation (state-regulation), and the prevailing practice of self-regulation, on the other.

In order to provide a theoretical framework for this regulatory-legislative environment, we present a simple model to depict the interdependencies between them. Figure 1 demonstrates this two-dimensional space with the two independent factors of self-regulation (the vertical axis) and legislation/state-regulation (the horizontal axis). The level of self-regulation and legislation can be interpreted as a continuum. A low level of self-regulation refers to
the situation when industry players (content providers and ISPs) do not pay any special attention to online safety issues. By contrast, a high level of self-regulation means that industry recognises the importance of online safety and, therefore, voluntarily (or by ‘soft’ pressure from governments) act against the negative, harmful issues.

As far as legislation if concerned, a low level signifies an undervalued and under-regulated legislative environment. In this case, the safety issues do not appear as necessities for either the regulator or political decision makers. This is illustrated by Palfrey’s first phase of the development of the internet when until the end of the 1990s online activities were below the radar of the state (Palfrey 2010). In 1998, the Children’s Online Privacy Protection Act in the United States marked the end of this period. Palfrey’s second “access denied” period began when states and governments started to think about online activities as something that needed to be blocked or heavily managed. It was a paradigm shift in legislation on children’s online safety. Therefore, a high level of legislation signifies that both regulators and political decision makers are sensitive to online safety.

Figure 1. Regulatory Environment for Industry’s CSR Activities

![Regulatory Environment for Industry’s CSR Activities](image)

The levels of CSR activities / self-regulation and legislation therefore define four different scenarios.
1. ‘Unregulated world’ refers to the situation where children’s online safety is simply not on the agenda of either regulatory policies or of industry (its self-regulatory and CSR practices). This can be thought of as a phase before online child safety becomes an important topic of social responsibility, i.e., the period from the early to mid-1990s. CSR activities of ISPs and network operators were non-existent or very limited in scope and magnitude. The separate domain of online content providers was almost unknown.

2. The scenario of ‘Low level of CSR’ appears when ISPs and content providers do not feel the necessity of proactive CSR or self-regulation, though governmental efforts have become alert to this issue. This more or less equates to Palfrey’s third period, the ‘access controlled’ phase. From the late 1990s, regulation in this area mushroomed in many European countries. Early examples dating from 2001 include the Czech Ministry of the Interior’s approval of the “Strategy of the Fight Against Information Technology Crime”; the Finnish Ministry of Transport and Communications began a campaign on safer chat; while the Belgian online reporting service (www.ecops.be) also began operations. In this early period, CSR activities were sporadic; initiatives were mostly individual experiments in awareness raising and education. International experience and knowledge transfer in CSR practices were also limited. Multinational corporate CSR strategies were also rare.

3. ‘Volunteering’ occurs when legislation is still weak, but some industry players act voluntarily to protect minors. In this scenario, CSR activities move ahead of the regulatory environment. In 2009, Hungarian Telekom’s internet content site [origo] launched its video playing and sharing site designed exclusively for children (Videa Kid) containing only child-appropriate content. In 2010, the company launched the free Content Lock service for its customers. By using this service, subscribers have the ability to control access to adult content. In this scenario there is a growing social need and corporate motivation for effective and visible CSR practices. “Doing something” in the field of online safety is formulated as an expectation of ISPs, network operators and content providers.

4. While examples exist for both of the previous two scenarios on a global scale (i.e. China, Middle-East, etc.), the situation in Europe and in the United States was a rather more smooth transition from low to high levels of both CSR activities/self-regulation and legislation. So finally, the fourth case scenario ‘Cooperative environment’ appears when both legislation and CSR activities/self-regulation appear to be high. By 2012, we see that the CSR strategies of a great number of network operators and ISPs
involve children’s online safety. Companies are developing programmes, campaigns and other tools to support this objective. The CSR practices of the industry and governments’ regulatory activities are head to head and mutually support each other. Professional organizations of the industry become more and more active in this field. For example, the European Telecommunications Network Operator’s Association (ETNO) has set up a specific Online Child Protection Task Team to monitor international developments and initiatives to collect information on and share best practices amongst members, and to communicate externally ETNO’s voluntary commitment to the cause.¹⁴

**Awareness and Protective Developments**

Taking a closer look at the available tools in both self-regulation and legislation, we see that they are quite similar. They include several forms of content filtering techniques (i.e. white and black lists, filtering and blocking) on the one hand, and awareness-raising and education type initiatives on the other. As an example, the “Principles for Safer Use of Connected Devices and Online Services by Children and Young People” produced by the industry-led alliance, the ICT Coalition, serves as a guideline here, because they cover many of the most recent issues in online safety. The principles and the basic tools are as follows:

1. Manage content – tools to manage access to certain content.
2. Parental controls – tools for parents to limit their children’s exposure to potentially inappropriate content and contact.
3. Dealing with abuse/misuse – tools for users to report content or behaviour which breaches someone’s interest.
4. Removal of child sexual abuse content – tools to remove the child sexual abuse content or illegal contact.
5. Privacy and control – tools to manage privacy settings appropriate for children and young people.
6. Education and awareness – tools to provide access to information that will help educate parents, teachers and children about media literacy and ethical digital citizenship.

These six principles/tools may be divided into two major groups. The first group includes all those kinds of education and awareness raising activities both in online and ‘traditional’ offline forms, while the second group includes providing tools for protection and improving the services available to support safer internet use.
In the first group of actions, the problems and potential threats and dangers of children’s online activities need to be promoted among children, parents, caregivers, teachers and other related social workers. Topics include: What are the concerns? What to do in case of being abused? How to report these events? How to defend minors? What are the techniques and methods that can be used to increase the level of security for children? In this complex web of actors, there is a constant need for education as technology continues to develop. And year on year, hundreds of thousands of young children start to use the internet, and incorporate more and more online activities into their daily lives as they get older (Livingstone, et al. 2010). As such, awareness raising and education is something that needs constant development and reflection.

Safer Internet Day, an initiative of the Safer Internet Programme and Insafe, has also provided ISPs and network operators with an opportunity to implement awareness raising campaigns across Europe. Some of these activities are realized in cooperation with national and local NGOs working in online safety. This also means that the effectiveness of these awareness raising and education initiatives also depends on the overall state of the civil society sector in a given country. Furthermore, in the case of some smaller countries (like for example Hungary) successful co-operation between industry and NGOs is often reliant on just a few enthusiastic and dedicated professionals.

The following activities of various European telecom and internet companies provide some examples of current educational and awareness raising CSR in children’s online safety:

- A tour around schools and Italian town squares to train children to make informed and responsible use of the internet and new media (Safe Browsing) which plans to involve at least one hundred thousand young students, teachers and adults (Telecom Italia).

- School campaigns – training of professors of computer science and Orange employee volunteers on internet safety for children to enable them to deliver awareness campaigns in schools, and supporting psychologists to give lectures in primary schools about safe internet usage (Orange).

- The opportunity for parents to have one-to-one live video discussion with experts on online safety (Orange).

- Congress for teenagers – sponsoring a congress dedicated to ‘Teenagers on the net’, where more than 1,000 young people participated (Orange).

- Volunteer education kit (‘Control Your Online Identity’) for teenagers designed to help them learn to protect their personal data online and reputation online. Internet safety coaching kit for teachers and adults working with children to raise awareness of internet safety and support meaningful and open dialogue with children on this topic, helping them
to recognize symptoms of cyberbullying, how to prevent online bullying from happening and how to intervene if it does (IBM).^{18}

- **BrukHue.com**, a school campaign based on participation and dialogue with teachers, students and their parents to raise awareness of the issue of digital bullying and to spread knowledge about which situations may lead to bullying and how to avoid these (Telenor Norway with Norwegian Red Cross, Childminder and the Norwegian Media Authority).^{19}

- **Employee volunteers** providing training for school children, teachers and parents associations on online safety. Employees are entitled to 3 days per year to volunteer time working on a good/charitable cause (Microsoft).^{20}

The second group of principles/tools include activities based on IT security and system improvements. Managing content, parental control tools, reporting abuse, content removal and managing privacy settings are mainly technology-driven projects supplemented by a necessary non-technological, back-office infrastructure. Practical outputs of these projects include hotlines, passwords, pop-up windows, deleting and blocking content, adjustable privacy and security level settings. Here, the role of ISPs and industry in general is not exclusive, since many tools are operated in conjunction with NGOs and government agencies. Some examples include:

- **Search engines** developed to provide safe content for children: such as fragFINN.de, a “smaller version” of the internet, an extensive list of websites that are both interesting and safe for children. Before a website is added to this “whitelist”, a team of media educators checks it against a set of strict criteria, ensuring that children have access only to websites suitable for them.^{21}

- **Child-friendly web pages**, special content developed for children: for example, egyszervolt.hu, a Hungarian website with a child-appropriate user-interface and carefully selected content, such as tales, rhymes, songs, games.

- **Internet hotlines** for reporting criminal content: for example the Internet Watch Foundation (http://www.iwf.org.uk/) (co-funded by the European Union) the aim of which is to minimize the availability of potentially illegal internet content.

- **Quality Control System**: for example, the Hungarian site www.bigyoo.hu which has a Quality Control System to evaluate the content based on required features, recommended features and exclusive factors.

- **Web Protection Software** for children: a wide variety of parental control software has been developed by ISPs, network operators and NGOs.
• URL blocking is the most “radical” and sometimes controversial method of protection, whereby a blacklist of forbidden URLs operates, based on police procedures or on the data of specialised organizations such as the Internet Watch Foundation (IWF).

These two groups of activities (awareness raising and education, and protective measures) can also be organized into a two-dimensional strategic space. Figure 2 demonstrates the possible scenarios.

**Figure 2.** Possible Strategic Actions of ISPs and Network Operators

![Diagram showing possible strategic actions of ISPs and Network Operators](image)

Here the vertical axis refers to awareness raising. A low level means that problems go unrecognised by society as well as by industry, whereas a high level represents a situation where children’s online safety is at the top of both industry’s and society’s priority list.

At an early stage, consumers’ internet use was primarily exploratory in nature. User attention was consumed by the rapid growth of content and services. It took some years both at the level of the individual user and the industry before more and more encounters and experiences with harmful content led to the realization that there is a dark side to the internet as well. As a result, user awareness supported by both objective and in many cases overreactive media attention began to rise. For industry, NGOs and governmental agencies (certainly with different levels of commitment and focus in their strategies), developing initiatives in awareness raising (i.e. media and educational campaigns) became an important part of their activities.
The horizontal axis on Figure 2 refers to levels of development of protection and cyber security. Here a low level marks weak or missing protection, and a high level represents a well-developed, smoothly functioning system of online safety tools. It was not so long ago that there were no child locks, logging, filtering, black and white lists, etc., and even the awareness of the consequences of too low a level of protection were unclear.

Using a simple matrix, the following scenarios can be identified comparing the levels of awareness raising and online protection.

1. *Unsafe environment* describes the situation (or period) when the importance of children’s online safety was low both at the level of society and industry, and the need for awareness raising and education was not on the agenda. Also, there were insufficient tools or applications for managing content or safety services for children. This phase of development can be viewed as the beginning period. In the mid-1990s, the internet was mostly the preserve of the early adopters and a few groups of professionals. It was far from reaching a critical mass both in terms of the number of users and available content and services. Harmful content certainly could be found online, but it posed little real danger to society (and especially to children) or to industry.

2. *Loud voices* is a condition where strong awareness raising meets ineffective protective tools: the regulatory environment is weak and the level of corporate responsibility is also low. This situation can be interpreted as the regulatory environment not matching the needs and expectations of society. This is a situation of under- or mis-regulation, where there are no real working tools for effective protection. From an historical perspective, ‘Loud voices’ could be considered as the seed phase of the late 1990s, when growing negative experiences and raising awareness of internet safety had come to the attention of different stakeholders (industry, governments, social scientists, etc.) The understanding of the nature of online risks and dangers was evolving, and scientific research started to focus on the societal effects of information technology use. However, effective regulation and functioning protective mechanisms were still missing. But the problem became evident at a larger societal level and public discourse started to grow stronger.

3. When the scenario of ‘*Underutilised opportunities*’ dominates, state regulation, political objectives become important, industry is providing usable tools for security, but awareness raising, the activities of civil society, and participation from users do not follow. This was the situation, for example, in the late 1990s, when (as a consequence of governmental legislation and pressure) companies were pushed to incorporate content-blocking into their browsers (i.e. Internet Explorer) in the United States, but users
were not really interested, prepared or motivated to use this function. Certainly, there is an overlap between the second and the third scenarios, since they do not follow each other in predetermined sequence. Different historical and political traditions in the roles of governments in regulation and in the social embeddedness of industry could lead to the dominance of one of the two middle scenarios.

4. The ‘Safer internet’ represents the co-existence and co-operation of state regulation, protective developments by industry and active awareness raising. These efforts mutually support one another. The initiative of the ICT Coalition (Principles for Safer Use of Connected Devices and Online Services by Children and Young People) demonstrates that major industry players have arrived at a stage where protective activities and CSR activities are both supporting the development of a safer online environment.

Conclusions

As we look at the development of legislation and CSR activities in respect of children’s online safety from a lifecycle management point of view, we can analyse this process using phases of evolution in time. The four stages of a typical life cycle are: (1) introductory stage, (2) the growth stage, (3) the stage of maturity and (4) saturation stage (Levitt 1965). These stages are consecutive as time goes by.

The self-regulation/legislation and the awareness raising/protective development spaces can be analysed by this evolution in time. The ‘unregulated world’ and the ‘unsafe environment’ scenarios of the two theoretical models can be interpreted as the initial, introductory stages of the 1990s and early 2000s. In the past few years, the situation in Europe is moving in an ever more linear fashion towards ‘safer internet’ and ‘cooperative environment’ scenarios. This constitutes a stage of maturity where both policy (at national and EU level) and industry (global and local level), supported by such domains as research on children’s internet use, media in general, and NGOs have more or less adequate knowledge and awareness when it comes to taking effective steps for a safer online environment, and finding the optimal balance between restriction and support.

Looking back at the development of provisions and activities around internet safety we can see also that in Europe there were no serious deviations from the imaginary diagonals (from the low left to the top right corner) of the two theoretical models introduced in this chapter. Legislation and self-regulation, and also awareness raising and protective developments both evolved ‘hand in hand’. Of course some national differences can be observed based mainly on
a country's available financial resources, the structure of the internet industry, general political traditions of state-economy relations, cultural and value differences on children and education, etc. But common policies at the level of the European Union and the global nature of the industry (a few dozen multinational corporations are dominating the whole value chain) make convergence a universal phenomenon across Europe. But the data also shows that there is a demand from users for more active safety tools and for the provision of information from ISPs and industry in general.

It remains the case that more sophisticated evaluation and better tools to measure and evaluate children’s online safety are still needed. There is a need for better indicators to measure the risks and harms children encounter online as well as to evaluate the effectiveness of the tools designed to protect them. Appropriate reporting and research needs to include hard and soft data at the same time, and requires input from all key stakeholders: industry players, state regulators and social science researchers.

Notes


2. In its 2006 recommendation the European Parliament and Council stated that the whole, self-regulation of the audio-visual sector was proving an effective additional measure, but it was not sufficient to protect minors from messages with harmful content and called for intensive cooperation between legislators, regulatory authorities, industry, associations citizens and civil society. (2006/952/EC) (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:378:0072:0077:EN:PDF)


9. The background of the story dates back to 2007 when one of the Belgian ISPs was ordered to install a filtering system to monitor all peer to peer traffic on its network and to block the exchange of files which were included in the repertoire of Belgian Society of Authors, Composers and Publishers (SABAM).


References

Chapter 9

The Influence of NGOs on Safer Internet Policy Making

Tatjana Taraszow

As an essential part of the multistakeholder process of internet safety, incorporating the experience and opinions of the large numbers of non-governmental organisations active in the field of online child protection is vital. This chapter examines the role of civil society and non-governmental organizations both in policy development and in implementation of internet safety. NGOs are, it will be shown, active in all phases of the policy process, from consultation all the way to legislation. It is important, therefore, to understand who these organisations represent and from whence they derive their legitimacy. Beginning with definitions and classification of NGOs, the chapter then analyses their contribution to creating a safer online world as well as the role they play within regulatory and policy processes at international, European, and national level.

Defining NGOs

The term “non-governmental organization” or NGO was created and came into use in 1945 when the first UN Charter was drafted because of the need for the United Nations to differentiate between its liaison with intergovernmental specialized agencies and international private organizations (Willets 2002). A broad variety of bodies and institutions are now described as NGOs. There is no generally accepted definition of NGOs and the term carries different connotations in different circumstances; thus definition and terminology vary widely. The NGO Global Network, a network of all non-governmental organizations associated with the United Nations, define NGOs as “non-profit, voluntary citizens’ group[s] which [are] organized on a local, national or international level” (NGO Global Network 2011). Two leading experts list the following key characteristics of NGOs: “formal, private, non-profit-distributing, self-governing, and voluntary” (Salamon & Anheier 1992: 134).
In sum, NGOs are non-governmental organizations, also known as civil society organizations, whose funds might be raised by the government. However, they maintain a non-governmental position, with no need for a government council.

NGO involvement in child protection has been prominent and extensive. Looking at the area of internet safety, there are three networks currently operating within the European context of online safety for children: (1) Insafe – a European network of Safer Internet Awareness Centres and Helplines, (2) INHOPE – the International Association of Internet Hotlines, and (3) eNACSO – the European NGO Alliance for Child Safety Online. Insafe and INHOPE are both multistakeholder networks comprising NGOs, for-profit-organizations, government bodies, industry, and universities whereas eNACSO exclusively comprises NGOs collaborating in child online safety. The role of each, is examined in further detail below.

**Involvement of NGOs in Insafe**

During the period 2010-2011, the 30 Safer Internet Awareness Centres of the Insafe network consisted of 70% public and 30% private entities (Insafe 2011), where universities, media institutes, governments, and education institutes were considered public entities while consumer protection organizations, business companies, internet service providers (ISPs) and various telecoms were considered private entities. The majority of the public organizations involved in Insafe were active in child protection (Figure 1) while among private organizations, different sectors were equally represented (Figure 2).

**Figure 1.** Types of Public Organizations Involved in Insafe; adapted from Insafe (2011)
In order to determine the involvement of NGOs in Safer Internet Centres within the Insafe network, a further analysis of data from Insafe was undertaken and participating organisations classified as: (1) NGO, (2) for-profit-organization, (3) governmental bodies, (4) industry, and (5) university. According to this analysis, NGOs are by far the largest group of organizations involved in the European Safer Internet network (60%), after government bodies (28%), and for-profit organizations (8%) (Figure 3).

**Figure 3.** Types of Organizations, i.e. NGOs, for Profit Organizations, Government Bodies, Telecommunication Industry, and Universities Involved in Insafe

- NGO: 60%
- Government: 28%
- University: 2%
- Industry: 1%
- For-profit: 8%
Involvement of NGOs in INHOPE

INHOPE currently has 42 members worldwide, of which nine are not Insafe members as they are located outside of Europe. Although an international association, INHOPE’s current focus lies on Europe, due to the fact that it originated in and is co-funded by the European Union. In order to investigate the involvement of NGOs in INHOPE, an equivalent analysis of participating organisations in Safer Internet Hotlines was carried out. Within INHOPE, the vast majority of hotlines are operated by NGOs (77.50%), followed by government bodies (15%) (Figure 4).

Figure 4. Types of Organizations, i.e. NGOs, For-profit Organizations, Government Bodies, Telecommunication Industry, and Universities Involved in INHOPE

Involvement of NGOs in eNACSO

The European NGO Alliance for Child Safety Online (eNACSO) was formed to create a unique network of individual NGOs to collaborate in the field of internet safety. eNACSO’s main aim is about policy advocacy in the areas of internet governance, keeping children safe online as well as strengthening children’s participation in policy development. The alliance emphasizes the important role and obligation of governments as well as European and international institutions to protect all children within their jurisdiction. Currently, the network consists of 25 children’s rights and child protection NGOs. 19 NGOs are ordinary members from 19 EU Member States, while six are associate members, five of which are from non-EU Member States (Table 1). The Alliance lacks transparency with respect to the procedure and requirements for membership as well as lacking transparency as to the rationale behind having only one member per country.
The latter might easily lead to the conclusion that eNACSO is reserved for an exclusive group of NGOs.

Table 1. List of Members and Associate Members of eNACSO

<table>
<thead>
<tr>
<th>NGO</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Members</strong></td>
<td></td>
</tr>
<tr>
<td>ECPAT</td>
<td>Austria</td>
</tr>
<tr>
<td>Our Child Foundation</td>
<td>Czech Republic</td>
</tr>
<tr>
<td>Save the Children</td>
<td>Denmark</td>
</tr>
<tr>
<td>Estonian Union of Child Welfare</td>
<td>Estonia</td>
</tr>
<tr>
<td>Save the Children</td>
<td>Finland</td>
</tr>
<tr>
<td>Action Innocence</td>
<td>France</td>
</tr>
<tr>
<td>Deutsche Kinderhilfe</td>
<td>Germany</td>
</tr>
<tr>
<td>Obrela</td>
<td>Greece</td>
</tr>
<tr>
<td>KÉK VONAL Foundation</td>
<td>Hungary</td>
</tr>
<tr>
<td>ISPCC</td>
<td>Ireland</td>
</tr>
<tr>
<td>Save the Children</td>
<td>Italy</td>
</tr>
<tr>
<td>Children Support Centre</td>
<td>Lithuania</td>
</tr>
<tr>
<td>Kanner Jugendtelefon</td>
<td>Luxembourg</td>
</tr>
<tr>
<td>ECPAT</td>
<td>Netherlands</td>
</tr>
<tr>
<td>Nobody’s Children Foundation</td>
<td>Poland</td>
</tr>
<tr>
<td>Instituto de apoio à Criança</td>
<td>Portugal</td>
</tr>
<tr>
<td>Save the Children</td>
<td>Romania</td>
</tr>
<tr>
<td>Protegeles</td>
<td>Spain</td>
</tr>
<tr>
<td>NSPCC</td>
<td>UK</td>
</tr>
<tr>
<td><strong>Associate members</strong></td>
<td></td>
</tr>
<tr>
<td>Media Education Center</td>
<td>Armenia</td>
</tr>
<tr>
<td>Innocence in danger</td>
<td>Germany</td>
</tr>
<tr>
<td>Stelit</td>
<td>Russia</td>
</tr>
<tr>
<td>Happy Kids Association</td>
<td>Turkey</td>
</tr>
<tr>
<td>International Children’s Center</td>
<td>Turkey</td>
</tr>
<tr>
<td>La Strada</td>
<td>Ukraine</td>
</tr>
</tbody>
</table>

Activity Sectors of NGOs Involved in Internet Safety

An analysis of the sectors in which the NGOs involved in internet safety are mainly active was undertaken. The International Classification of Nonprofit Organizations (ICNPO) as a standard classification was used to identify the activity sectors of the 107 NGOs involved in Insafe, INHOPE, and/or eNACSO. Most of the NGOs involved in any of the three networks can be classified into one of the four ICNPO groups: (a) Education and Research, (b) Social Services, (c) Law, Advocacy and Politics, or (d) Business and Professional Associations, Unions (Figure 5). More than 30% belong to the area of Law, Advocacy and Politics (Table 2), out of which 25% are advocacy organizations “that protect the rights and promote the interests of specific groups of people” (Salamon et al. 1999: 474) – mostly the rights and interests of children whereas 4% are civic associations that “encourage and spread civic mindedness” (Salamon et
al 1999: 474) and 3% provide services to victims of crime, i.e. advice, support, counselling. 28% of the NGOs belong to the area of Education and Research; 25% of these organizations focus on education, 3% focus on research (Table 2). Some of these organizations were specifically launched for awareness raising and educational activities such as safe use of the internet or to fight inappropriate and illegal content online. For example, Childnet International was established with the aim of making the internet a safe place for children by promoting interaction between the different sectors involved. In the UK, the Internet Watch Foundation emerged as an internet hotline from the Safety Net Foundation following agreement between the foundation and relevant government, police, and internet service provider stakeholders. Protégeles in Spain similarly emerged to fight child pornography and improve children’s safety online through campaigns.

Figure 5. Activity Sectors of NGOs Involved in Insafe, INHOPE, and/or eNACSO According to the ICNPO system

Another 25% of the NGOs involved in Insafe, INHOPE, and/or eNACSO were classified as Social Services comprising the sub-categories ‘child welfare’, ‘family services’, and ‘self-help/personal counselling’ (Table 2). 13% of the organizations involved in Insafe, INHOPE, and/or eNACSO are classified as Business and Professional Associations, and Unions (Table 2). Several ISP associations are not only actively involved in Insafe but also in INHOPE by operating a hotline to anonymously report abusive or illegal online material, for example those in Austria, France, Ireland, and Latvia. The reason for this might be a recent EC policy supporting nodes that combine a Safer Internet Awareness Center and a Hotline within the same organization, be it ISPs or
NGOs. It is worth noting that many of the organizations in Insafe, INHOPE, and/or eNACSO participating NGOs are well-known European or international organizations, including ECPAT, the International Centre for the Missing and Exploited Children (ICMEC), Save the Children, and PEGI.

## Policy Influence of NGOs

### Global Level

Because the internet is a global medium, a key role is played by international organizations and intergovernmental initiatives such as the International Telecommunications Union (ITU) and Internet Governance Forum (IGF) in establishing and maintaining a safe global online environment. Despite the lack of internationally binding regulations and laws and given the sometimes competing nature of national interests, civil society groups have been to the fore in pushing forward the agenda of online safety.

IGF is one of the high profile opportunities for NGOs to contribute to the policy process. According to the summary of IGF's history by de Bossy (2005), its origins lie in the two sessions of the World Summit on the Information Society (WSIS) organised by the ITU in 2003 and 2005. After the 2003 summit failed to agree on the future of internet governance, the Working Group of Internet Governance (WGIG) was established in order to investigate and propose actions by the second WSIS in 2005 (de Bossey 2005). The WGIG was the first working group on internet safety of its kind and comprised a mixture of 40 representatives from governments, the private sector, academia, and civil society (de Bossey 2005). During its two year existence, the WGIG developed and proposed four models in their final report, basically recommending the creation of a new UN-linked space for dialogue between all

### Table 2: Results of the Detailed Research Identifying the Activity Sectors of NGOs Involved in Insafe, INHOPE, and/or eNACSO Using ICNPO Classes and Sub-categories

<table>
<thead>
<tr>
<th>ICNPO class</th>
<th>Sub-categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 300</td>
<td>Other</td>
</tr>
<tr>
<td></td>
<td>Education</td>
</tr>
<tr>
<td></td>
<td>ICT education 25%</td>
</tr>
<tr>
<td></td>
<td>Internet education 10%</td>
</tr>
<tr>
<td></td>
<td>Other education 15%</td>
</tr>
<tr>
<td>2 400</td>
<td>Research 3%</td>
</tr>
<tr>
<td>4 100</td>
<td>Social services 25%</td>
</tr>
<tr>
<td></td>
<td>Child welfare 18%</td>
</tr>
<tr>
<td></td>
<td>Family services 2%</td>
</tr>
<tr>
<td></td>
<td>Self-help 5%</td>
</tr>
<tr>
<td>7 100</td>
<td>Civic &amp; advocacy organizations 29%</td>
</tr>
<tr>
<td></td>
<td>Advocacy organization 25%</td>
</tr>
<tr>
<td></td>
<td>Civic association 4%</td>
</tr>
<tr>
<td>7 200</td>
<td>Law &amp; legal services 3%</td>
</tr>
<tr>
<td></td>
<td>Victim support 1%</td>
</tr>
<tr>
<td></td>
<td>Consumer protection 2%</td>
</tr>
<tr>
<td>11 100</td>
<td>Business associations 13%</td>
</tr>
</tbody>
</table>
relevant stakeholders on an equal basis, thus reducing the then-dominance of the US in international internet governance, in particular through the American Internet Corporation for Assigned Names and Numbers (ICANN) (de Bossey 2005). The broadest of these, Model 4, recommended the establishment of three new bodies to support inter-governmental cooperation: (1) a Global Internet Policy Council to supervise the private sector’s activities, (2) a World Internet Corporation for Assigned Names and Numbers for the operational functioning of the internet, and (3) a forum for public-private policy discussions through the Global Internet Governance Forum. Agreement was reached during the second WSIS in 2005 to create the IGF, hence only taking into account one part of WGIG’s proposed Model 4. Since its establishment, the IGF is one of two unique international organisations providing a forum for multi-stakeholder policy dialogue on internet governance on a global level. As a forum without membership, IGF holds yearly meetings across the world; it has established a Multistakeholder Advisory Group and supports several regional and local initiatives and coalitions – all with the purpose of discussing, advising and where possible agreeing key policy elements of internet governance among all stakeholders to create a safer online environment globally.

The Family Online Safety Insitute (FOSI) is another international non-profit organisation active in internet safety. FOSI is a membership-based organization with membership fees. Although FOSI claims to bring together all internet safety stakeholders, including industry, government, NGO, academia, and media, to make the online environment a safer place for children, NGOs, academia, and government are clearly underrepresented in the membership pool.5

European Level

The European Union has played a central role in establishing a common agenda for internet safety within Europe. In 1999, the European Parliament and Council launched “a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks” (European Parliament, Council 1999: 1) as the principal platform for multistakeholder involvement in promoting safer use of the internet and other communication technologies. This plan came to be known as the Safer Internet Action Plan covering activities during the period 1999 to 2004. Building on its predecessor’s aim, the Safer Internet Plus programme, adopted in 2005 by the EC, broadened its scope to also include new online technologies as well as to combat racism and spam (European Parliament, Council 2005). The thereafter adopted Safer Internet Programme from 2009 to 2013, added emerging issues of online grooming and cyber-bullying (European Commission 2012c). Within the Safer Internet Programme, the Commission co-funds projects contributing to a safer internet across five different sectors: (1) awareness raising, (2) fight
against illegal content, (3) filtering and content labeling, (4) research, and (5) involvement of civil society. In total, during the period 2009-2012, the Safer Internet Programme has co-funded 16 projects actively involved in internet safety policies with the majority belonging to the topics “fight against illegal content” (6 projects) and “research and training” (5 projects) (Table 3).

**Table 3.** Involvement of NGOs, For-profit Organizations, Government Bodies, Telecommunication Industry, and Universities in the Safer Internet Programme of the European Commission (2009-2012)

<table>
<thead>
<tr>
<th>Project</th>
<th>NGO</th>
<th>For-profit organization</th>
<th>Government body</th>
<th>Telecommunication industry</th>
<th>University</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Safer Internet Centers</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>InSafe</td>
<td>53</td>
<td>7</td>
<td>25</td>
<td>1</td>
<td>2</td>
<td>88</td>
</tr>
<tr>
<td><strong>Fight against Illegal Content</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>INHOPE</td>
<td>31</td>
<td>2</td>
<td>6</td>
<td>0</td>
<td>1</td>
<td>40</td>
</tr>
<tr>
<td>Interpol</td>
<td>0</td>
<td>0</td>
<td>190</td>
<td>0</td>
<td>0</td>
<td>190</td>
</tr>
<tr>
<td>CIRCAMP</td>
<td>0</td>
<td>0</td>
<td>11</td>
<td>0</td>
<td>0</td>
<td>11</td>
</tr>
<tr>
<td>I-Dash</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>FIVES</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>MAPAP</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>34</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>209</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>8</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>256</td>
</tr>
<tr>
<td><strong>Filtering and Content Labeling</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIP-BENCH 2</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>PEGI Online</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Quatro Plus</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>22</td>
</tr>
<tr>
<td><strong>Research &amp; Training</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ROBERT</td>
<td>0</td>
<td>0</td>
<td>12</td>
<td>0</td>
<td>0</td>
<td>12</td>
</tr>
<tr>
<td>EU NET ADB</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>POG</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>EU Kids Online</td>
<td>3</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>28</td>
<td>33</td>
</tr>
<tr>
<td>EU Kids Online II</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>42</td>
</tr>
<tr>
<td><strong>Civil Society Involvement</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>64</td>
</tr>
<tr>
<td>eNACSO</td>
<td>25</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>122</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>19</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>252</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>54</td>
</tr>
</tbody>
</table>

Within the Safer Internet Programme, NGOs are the second biggest group of entities after government bodies – mainly police or law-enforcement organizations – with involvement in making the internet a safer place through awareness raising, tool development, cross-country cooperation, product labeling and content filtering, as well as research (Figure 6). Thus, across the 16 projects of the Safer Internet Programme, 122 NGOs are actively engaged in contributing to the Commission’s policy of “making the internet a safer place for Europe’s children” (European Commission 2012c), equivalent to 27% of all participating entities.
Public Consultations and NGOs

One of the ways in which NGOs exert influence on the policy process is by participation in public consultations, both those organised by the European Commission as well as those organised by national governments. Public consultations have been a central feature of the policy making process whereby submissions are invited from public authorities, companies, industry, NGOs, as well individual citizens. Since 2003, a total of 84 public consultations were hosted by the European Commission’s Information Society thematic portal out of which three were related to the Safer Internet Programme and thus directly focused on online technologies and safety: “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 (European Commission 2012c). Other relevant European programmes have included topics such as broadband networks, open internet and net neutrality, roaming and ePrivacy (European Commission 2012b).

With respect to those public consultations thematically related to the Safer Internet Programme, an analysis was undertaken of the different kinds of organizations who responded. Almost 40% of the organizations who responded were classified as NGOs (Figure 7). A third of these NGOs represented business and professional associations of mobile operators, mobile services, ISPs, (entertainment) software developers, enterprises, and publishers. The second largest group of organizations participating in the above mentioned public
contributions (23%) and included various local Safer Internet Awareness Centres, Hotlines, EU Kids Online, INHOPE as well as individuals; this group is summarized under the ‘other’ category. For-profit enterprises and governments/authorities were equally involved with 16% and 13%, respectively. National mobile operators and ISPs were less actively involved with 8% (industry). The least involved entity in public consultations about safer internet issues is the educational sector, universities in particular, with less than 2%.

Figure 7. Distribution of types of Organizations, i.e. NGOs, For-profit Organizations, Government Bodies, Telecommunication Industry, and Universities, Involved in Public Consultations Launched by the Safer Internet Programme of the European Commission between 2006 and 2008

Contributions to policy draft documents in the form of providing recommendations in public consultations does not, of course, necessarily lead to policy influence or change. An example of where NGOs were less than successful in influencing policy was in relation to the 2011 Directive on combating the sexual abuse and sexual exploitation of children and child pornography. The new Directive allowed for EU legislation on child protection on a transnational basis, and replaced a Council Framework Decision from 2004, to take into account new developments and challenges related to online and mobile technologies (European Parliament, Council 2011). Six prominent children’s rights organizations – UNICEF, ECPAT, Safe the Children, Missing Children Europe, eNACSO, and NSPCC – along with Europol and Interpol made strong recommendations on some of its key provisions. For instance, the group argued strongly in favor of three issues of utmost importance: (1) to make it compulsory for Member
States to block child pornography websites without prior judicial authorization by an independent body (Article 21); (2) to include offline grooming as well as children over the age of sexual consent within the definition of ‘solicitation of children for sexual purposes’ (Article 6); and (3) to include mandatory screening checks for employers when recruiting professionals and volunteers regularly and directly engaged with children (Article 10) (eNACSO 2011). However, none of these recommendations made it into the final version of the Directive “on combating the sexual abuse and sexual exploitation of children and child pornography” (European Parliament and Council 2011: 1).

Local Level
In order to investigate whether a high degree of NGO influence in safer internet policy making leads to a high degree of “public discourse on children’s internet use and possible risks of the internet” (Hasebrink, Livingstone, Haddon, & Ólafsson 2009: 7), EU Kids Online examined the influence of NGOs on ICT regulation and related policies. The results indicate two types of countries with NGO influence: strong and weak (Table 4). Alongside NGOs’ degree of influence, press freedom is another indicator of a country’s regulatory framework, based on the assumption that civil society shows greater participation in policy making in countries with a high degree of press freedom. Indices of press freedom derived from Reporters Without Borders (2012) are therefore also used as an indicator of NGO involvement and compared to the degree of NGO influence (Table 4).

<table>
<thead>
<tr>
<th>Table 4.</th>
<th>Countries Classified According the Local Degree of NGO Influence, Based on Analysis Results of EU Kids Online (Hasebrink et al. 2009) and Based on the Degree of Press Freedom (Reporters Without Borders 2012)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Strong NGO influence</strong></td>
<td><strong>Weak NGO influence</strong></td>
</tr>
<tr>
<td>Austria</td>
<td>Bulgaria</td>
</tr>
<tr>
<td>Belgium</td>
<td>Cyprus</td>
</tr>
<tr>
<td>Denmark</td>
<td>France</td>
</tr>
<tr>
<td>Estonia</td>
<td>Greece</td>
</tr>
<tr>
<td>Germany</td>
<td>Portugal</td>
</tr>
<tr>
<td>Iceland</td>
<td>Sweden</td>
</tr>
<tr>
<td>Ireland</td>
<td></td>
</tr>
<tr>
<td>Italy</td>
<td></td>
</tr>
<tr>
<td>Netherlands</td>
<td>Ireland</td>
</tr>
<tr>
<td>Norway</td>
<td>Sweden</td>
</tr>
<tr>
<td>Slovenia</td>
<td></td>
</tr>
<tr>
<td>Spain</td>
<td></td>
</tr>
<tr>
<td>UK</td>
<td></td>
</tr>
</tbody>
</table>
Combining both indicators of NGO involvement at the local level reveals the following four country profiles: (1) weak NGO influence and low press freedom, (2) weak NGO influence and high press freedom, (3) strong NGO influence and low press freedom, and (4) strong NGO influence and high press freedom. Thus, the two separate classification systems of countries according to either the influence of NGOs or degree of press freedom were linked in order to provide a new classification system (Figure 8).

In order to test the combined indicator, two illustrative hypotheses were investigated with respect to the three above mentioned public consultations related to the Safer Internet Programme: (a) that the number of total contributions from NGOs is highest in the category of strong NGO influence and high press freedom; and (b) that the number of countries involved in providing contributions is highest in the category of strong NGO influence and high press freedom.

The results of the initial analysis indicate positive support for both hypotheses: (Figure 9) (a) 22 contributions were made from NGOs located in countries with high NGO influence and high press freedom—the highest number; and (b) NGOs from 10 countries with strong NGO influence and high press freedom participated in the consultations. However, it seems that both assumptions do not hold true for all countries. For example, the assumption that NGOs from all countries with strong NGO influence and high press freedom (such as Austria,
Estonia, and Norway) participate in EU public consultations turns out not to be the case. Similarly, the assumption that NGOs from countries with weak NGO influence and low press freedom are not involved in public consultations does not apply to France and Greece where NGOs are actively involved.

To summarize, European countries may be compared with regard to their NGO participation in policy making on safer internet issues based on their level of NGO influence (Hasebrink, et al. 2009) as well as their press freedom index (Reporters Without Borders 2012), the combination of which provides a combined taxonomy that may be applied to various NGO activities such as participation in public consultations of the EU (Table 5).

Moreover, according to the number of policy contributions to the EU Safer Internet Programme, some NGOs are more active than others in policy influence, i.e., participated more than once at public consultations and thus show a higher involvement in policy making (Table 6). NGOs from ‘old’ EU Member States tend to be more actively involved in policy making, with the UK as the leading country.

The combined results of the EU Kids Online network and the results presented above indicate that at European level some countries with specific NGOs participate more actively at the policy level than others. Countries with higher participation are Belgium, France, Germany, Greece, Ireland, Italy, Poland, Portugal, Spain, and UK.
In sum, civil society organizations such as NGOs, associations, networks, or alliances, do the best they can under given circumstances to provide recommendations to governments and public bodies in order to influence and shape national or transnational policies. Regardless of their motivation, enthusiasm,

Table 5. Comparison of Countries’ Participation in Safety Internet Policy through EU Consultations Based on Four Different Approaches

<table>
<thead>
<tr>
<th>High NGO Involvement</th>
<th>High press freedom</th>
<th>High NGO involvement &amp; high press freedom</th>
<th>Participation in EU’s public consultations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Austria</td>
<td>Austria</td>
<td>Austria</td>
<td>Belgium</td>
</tr>
<tr>
<td>Belgium</td>
<td>Belgium</td>
<td>Belgium</td>
<td>Cyprus</td>
</tr>
<tr>
<td>Denmark</td>
<td>Cyprus</td>
<td>Denmark</td>
<td>Denmark</td>
</tr>
<tr>
<td>Estonia</td>
<td>Czech Republic</td>
<td>Estonia</td>
<td>France</td>
</tr>
<tr>
<td>Germany</td>
<td>Denmark</td>
<td>Germany</td>
<td>Germany</td>
</tr>
<tr>
<td>Iceland</td>
<td>Estonia</td>
<td>Iceland</td>
<td>Greece</td>
</tr>
<tr>
<td>Ireland</td>
<td>Finland</td>
<td>Ireland</td>
<td>Ireland</td>
</tr>
<tr>
<td>Italy</td>
<td>German</td>
<td>Netherlands</td>
<td>Italy</td>
</tr>
<tr>
<td>Netherlands</td>
<td>Iceland</td>
<td>Norway</td>
<td>Netherlands</td>
</tr>
<tr>
<td>Norway</td>
<td>Ireland</td>
<td>UK</td>
<td>Spain</td>
</tr>
<tr>
<td>Slovenia</td>
<td>Luxembourg</td>
<td></td>
<td>UK</td>
</tr>
<tr>
<td>Spain</td>
<td>Netherlands</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UK</td>
<td>Norway</td>
<td>Poland</td>
<td>Slovakia</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sweden</td>
<td>UK</td>
</tr>
</tbody>
</table>

Table 6. Names of NGOs and the Country of Their Establishment that Provided More than One Contribution to Public Consultations of the EU’s Safer Internet Programme

<table>
<thead>
<tr>
<th>NGO</th>
<th>Country</th>
<th>Number of contributions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Research and Information Centre of the Belgian Consumer Organizations (CRIOC)</td>
<td>Belgium</td>
<td>3</td>
</tr>
<tr>
<td>Forum des Droits sur l’Internet (FDI)</td>
<td>France</td>
<td>2</td>
</tr>
<tr>
<td>Stiftung Digitale Chancen</td>
<td>Germany</td>
<td>3</td>
</tr>
<tr>
<td>Consumer’s Protection Centre (KEPKA)</td>
<td>Greece</td>
<td>2</td>
</tr>
<tr>
<td>Anchor Youth Centre</td>
<td>Ireland</td>
<td>2</td>
</tr>
<tr>
<td>Associazione Difesa Consumatori e Ambiente (ADICONSUM)</td>
<td>Italy</td>
<td>3</td>
</tr>
<tr>
<td>Protegeles</td>
<td>Spain</td>
<td>2</td>
</tr>
<tr>
<td>Childnet International</td>
<td>UK</td>
<td>3</td>
</tr>
<tr>
<td>Children’s Charities’ Coalition on Internet Safety (CHIS)</td>
<td>UK</td>
<td>2</td>
</tr>
</tbody>
</table>
and effort it is neither clear nor obvious given the lack of transparency if the offered consultations are actually taken into consideration or even adapted for the relevant policy.

The Relationship Between NGOs and Industry

One important set of relationships within the multistakeholder field of online safety is that between the NGO sector and industry. Over the past decade, the trend of NGOs working collaboratively with companies has developed significantly. Both civil society and industry sectors have acknowledged the importance of mutual cooperation. NGOs, in particular, have recognized the positive value of including industry stakeholders such as ISPs, mobile operators, or content providers within online safety initiatives. Companies, on the one hand, have noted the importance of online safety as an aspect of corporate social responsibility. Moreover, large internet companies have the resources to effect real change. At the same time, private sector companies might not necessarily have the expertise to carry out awareness-raising projects, something that NGOs have in abundance though often without the means to put their expertise into practice. As such, partnerships and collaboration between NGOs and industry stakeholders characterize a smart solution.

In its latest strategy for a better internet for children, the European Commission has requested the industry sector to “develop and offer targeted, interactive quality content for children, as well as user friendly tools that encourage their creativity and help them learn” (European Commission 2012a: 7) as well as to “provide funding and technical support to NGOs and education providers for the development of resources” (European Commission 2012a: 9). This represents a further area where NGOs can collaborate and support industry’s efforts. It also underlines the Commission’s objective of supporting alliances between civil society and industry. Previous initiatives and internet safety networks, co-funded by the Safer Internet Programme, have established partnerships with content providers or telecommunications companies. For example, in 2010, Insafe set up a collaboration with Liberty Global, Microsoft, and Vivendi (Insafe 2010). One year later, Insafe managed to initiate cooperation with several more institutions from the industrial sector such as Facebook, Microsoft, and Kaspersky Lab (Insafe 2011). Eight of the thirty Insafe Awareness Centers now work in collaboration with either for-profit companies or industry stakeholders or both. Moreover, both umbrella organizations, CHIS and eNACSO, liaise with the internet industry when recommending policy improvements at local and European level, respectively. The two global UN-based platforms, WSIS and IGF, provide a space for networking, establishment of partnerships, visibility to activities and projects, as well as communication among all relevant
THE INFLUENCE OF NGOS ON SAFER INTERNET POLICY MAKING

stakeholders. Also, FOSI as an international, non-profit organization encourages collaboration between the different sectors through research, activities, and policy recommendations. Moreover, FOSI itself participates on a consultative basis in two advisory boards to Facebook and Norton – two major companies for whom online safety is an important issue. Yet, with this strategy in mind, the range of partnerships supported through the Safer Internet Programme so far, does not fully realize the potential of cross-sectoral collaboration. Out of a total of 445 entities supported under the Safer Internet Programme, only one belongs to the industry sector and only 19 to the for-profit sector.

Despite good intentions, partnerships between NGOs and companies, coming from very different backgrounds, face substantial challenges and there is no one model for success (Table 7) (Damlamian 2006).

Table 7. Possible Problems and Challenges Arising Before the Establishment or During the Execution of a Partnership Between the Civil Society Sector and Business Sector

<table>
<thead>
<tr>
<th>Challenges at NGO side</th>
<th>Challenges at company side</th>
<th>Challenges at both sides</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weak organization</td>
<td>Convinced to impose an action plan instead of developing a common road map</td>
<td>“internal schizophrenia”: internal disagreement about desired type of interaction with other partner</td>
</tr>
<tr>
<td>Unclear goals, expectations, and visions</td>
<td>Lack of sincere dedication to partnership and its goals</td>
<td>Lack of long-term goals and benefits of partnership</td>
</tr>
<tr>
<td>Staff’s relative inexperience in dealing with the corporate world and their lack of professional expertise</td>
<td>Corporate social responsibility not part of the business culture, thus no understanding or support by employees</td>
<td>Lack of understanding of other party’s interests and needs</td>
</tr>
</tbody>
</table>

Note: Adapted from Damlamian (2006)

In addition, a further, crucial challenge lies in the fact that NGOs often seek financial support from industry stakeholders with implications for the essential values of transparency and accountability that legitimate NGOs. Given that civil society organizations operate under public laws and regulations, they need to follow standards of accountability and transparency to ensure that the interests of the general public are served and these organizations do not violate the public’s trust (Democracy Web, n.d.).

To sum up, various relationships between NGOs and companies to promote a safe online world have been established not only in Europe but worldwide.
The current trend is to further support such partnerships. However, some caution must be exercised. Before agreeing to a partnership, both partners should be aware of their own limitations, the other's history, needs, and interests as well as be open-minded to jointly agree on goals, frameworks, time lines, etc. Having done so, the partnership will be better able to deal with evolving challenges, and consequently all partners involved will benefit equally.

Conclusions

From this review of the role of NGOs in internet safety policymaking, a number of recommendations arise. Firstly, at the global level, greater involvement of civil society in the policy process could be promoted by international organizations such as the IGF or ISOC. Besides international involvement civil society should increase its involvement also at the local and regional level. Currently, governmental bodies, researchers, and the industry sector are well represented; however, civil society is very underrepresented. Details of all participating entities should be publicly available, preferably in English, to guarantee transparency. Moreover, network meetings should be encouraged to publish statistics regarding participants and presenters, thus providing data that can then be used as indicators of multi-stakeholder involvement in internet safety. There is also a need to establish an international NGO representative organization at the global level comparable to eNACSO at the European level. Such an organization could then seek to promote greater participation of NGOs in global internet networks.

There is also a need to strengthen relationships between the sectors of law enforcement, civil society/NGOs, and industry within existing networks in the digital safety sphere. Specifically, better cooperation between (a) law enforcement agencies (Interpol, CIRCAMP, VGT, etc.), (b) initiatives focused on education (FOSI, Insafe, eNACSO, etc.) and child welfare (UNICEF, Save the Children, ICMEC, ECPAT, World Vision, etc.), and (c) global telecommunication associations such as GSMA. Moreover, these should be fostered through platforms such as the ITU at a global level, or through the European Commission.

Secondly, at the European level, the example of eNACSO demonstrates the value of an umbrella organization combining expertise, resources, and possibly impact on the field of internet safety. eNACSO is a good start; however, it includes only a small selection of all active initiatives in this area. Either eNACSO could work towards becoming such an umbrella network or the Safer Internet Programme of the Commission should add this point to its policy agenda under the heading of ‘involving European civil society’ by creating and offering funding opportunities to initiate such an umbrella organization. With respect to the EC’s policy of involving the civil society sector, further support is needed to strengthen civil society involvement. Furthermore, a clear distinction is needed
between involving civil society and involving as many relevant stakeholders as possible (European Commission 2012c). While such an objective is admirable, in practice this does not seem to be happening. According to the results presented in this chapter, only Insafe tries to include all stakeholders; but not a single Safer Internet Awareness Centre has members from all stakeholder groups. Likewise, it might be useful to launch a network comprised of all European and possibly global Helplines as already exists for Hotlines with INHOPE and for Awareness Centres with Insafe. Again, the Safer Internet Programme is in a good position to take the lead by adding this point to its policy agenda and supporting its implementation.

In general, it can be concluded that NGOs and other civil society organizations are of utmost importance for the implementation of initiatives, for disseminating internet safety, and for contributing to effective policy on vulnerable populations. Similarly, partnerships with industry are of significance, particularly when they are jointly developed, planned, and executed. The general aim, whether at a global, European, or local level, should be smooth collaboration between the three pillars of civil society, government, and industry not only to ensure the involvement and participation of all relevant stakeholders but also to jointly develop, implement, and evaluate policies needed to create a safer online world for children and adults alike.

Notes
1. Ministries and entities such as Media Authorities, Media Councils, and/or Media Classification Boards were combined in the category called ‘government body’.
2. The challenge here was to clearly identify the type of each partner organization of all Safer Internet Centres despite lack of respective information at Insafe’s website as well as language barriers at the Safer Internet Centres’ websites. Therefore, a second step was introduced during the process of data collection during which project managers and coordinators of each Safer Internet Centre were contacted to verify the respective data collected. The data of 14 Safer Internet Centres was verified.
3. Due to the same challenges as described above the second step during data collection of contacting hotline managers and coordinators was used to verify the respective data collected. The data of 14 hotlines was verified.
4. ICNPO is a generally accepted classification. ICNPO originates from a team of scholars working on the Johns Hopkins Comparative Non-Profit Sector Project Phase II covering 22 countries in Europe, Asia, Latin America, and North America (Salamon, Anheier, List, Toepler, Sokolowsko, and Associates, 1999)
5. The current FOSI members include: AOL, AT&T, BAE Systems Detica, BT Retail, Comcast, Disney, Entertainment Software Association, Facebook, France Telecom, Google, GSM Association, Microsoft, Mind Candy, Motion Picture Association of America, NCTA, Nominum, Sprint, Symantec, Time Warner Cable, Telefónica, The Cyber Guardian, The Wireless Foundation, Verizon, and Yahoo!
6. It was not possible to categorize all EU countries due to lack of classification of the type of NGO influence, i.e. strong or weak, by the EU Kids Online network.
7. Czech Republic (1 contribution), Finland (1 contribution), and Poland (2 contributions) could not be categorized due to missing information regarding their NGO influence
8. Contributions of organizations belonging to ICNPO class 11 were not taken into account.

References


Chapter 10

Teaching Internet Safety,
Promoting Digital Literacy

The Dual Role of Education and Schools

Brian O’Neill & Yiannis Laouris

Policy recommendations in the area of young people’s use of the internet frequently point to education as central to the challenge of improving internet safety. While the primary responsibility for ensuring children’s safety online is assumed to be a parental one, it is recognised that parents may not always be sufficiently informed or competent to be the primary source of internet safety education for their children. Industry and a variety of safer internet organisations are also active players in internet safety messaging but it is to the school, more often than not, that policy makers look to ensure that all children have access to basic information about protecting themselves online. As early as 1996, the European Union’s Green Paper On The Protection Of Minors And Human Dignity In Audiovisual And Information Services (European Commission 1996) recognized formal education as central to promoting internet safety and proposed close cooperation with the educational community to develop the necessary teaching materials to fulfil this task. In 2009, following an audit of schools-based internet safety education, the Safer Internet Programme called for online safety to be a core subject from as early an age as possible (European Commission 2009). In addition, safe and responsible use of the internet is seen as central to the digital competence and, more widely media literacy, considered essential to young people’s welfare in the information society (Ala-Mutka, Punie and Redecker 2008). Key reference points within European media policy – the Recommendation on Protection of Minors and Human Dignity (2006) the Audiovisual Media Services Directive (2007) – cite media literacy education as crucial for developing young people’s responsible use of audiovisual and on-line information services. With the call by the European Commission in its strategy for a better internet for Member States to include teaching online safety in school curricula by 2013 (European Commission 2012: 8), education is to the fore in internet safety efforts as never before.

This chapter addresses two aspects of the challenge facing educationalists as they seek to meet these ambitious demands. Firstly, in stepping up efforts
to deliver online safety in schools, what core messages should it incorporate and how can it be best implemented within an already busy school curriculum? Drawing on data from EU Kids Online as well as European Commission research into provision for online safety education, we discuss the very diverse settings and target age groups that currently exist across Europe and the problems that arise in defining minimal standards. Secondly, to be sustainable online safety education has to be more than a list of ‘dos and don’ts’; it needs to foster media literacy and greater digital citizenship, as commentators have argued (Passey 2011). Yet, what precisely this might involve and the implications for schools and for young people, remain unclear. What do educators need to do and what support do they require to lead such an educational transformation? More to the point, how does it take account of internet safety messaging and does it alter the balance between protection versus empowerment?

**Teaching Internet Safety**

The pivotal role of schools in internet safety education was underlined in the first phase of EU Kids Online. Reflecting on the available evidence of online risks for children and young people, the final report argued that:

> Schools are best placed to teach children the digital and critical literacy skills required to maximise opportunities and minimise risks. Schools are also best placed to reach all children, irrespective of socioeconomic status and other forms of inequality. For both these reasons, schools have a key role to play in encouraging and supporting creative, critical and safe uses of the internet, crucially throughout the curriculum but also at home or elsewhere. (Livingstone and Haddon 2009: 23).

However, in order to fulfil this objective, schools themselves must be ICT-rich environments and suitably equipped to provide an environment in which to teach digital literacy. According to the EU Kids Online survey of 9-16 year old children across Europe, the child’s school is the second most common location for going online (63%) after the home (87%), providing children with important access opportunities (see Figure 1). In countries such as the Netherlands, Denmark, Norway, Finland, and the United Kingdom, over 80% of all 9-16 year old children access the internet at school. But the picture is uneven and in many countries, only a half of all internet-using children have access (Slovenia, Belgium, France, Germany, Romania). Notably, a third or less have access to the internet at school in Italy and Greece, thereby placing significant limits on their capacity to act as digital educators.
EU Kids Online found that 58% of young people had received internet safety advice from teachers (compared to 63% from parents and 44% from peers) (Livingstone, et al. 2011). Parents also identified schools as their preferred source of information about internet safety. While most parents say they get internet safety information from family and friends (48%) rather than from their child’s school (27%), when asked where they would prefer to get such information, it was the school that was identified as the most desired source (43%), followed by mainstream media (32%), family and friends (29%) and internet service providers (26%) (Livingstone, et al. 2011: 129).

According to the children interviewed in the survey, their teachers had engaged with them in some aspect of internet safety, such as explaining why some websites are good or bad (58%), recommending ways to use the internet safely (58%), talking about what children do online (53%), and suggesting ways to behave with other people online (48%). Most teachers also made rules about what children could do on the internet in school (62%) though fewer intervened when children reported something online had upset or bothered them (24%). Indeed, the role of teachers overtakes that of parents for older teenagers and for children from lower SES homes (Pasquier, Simões and Kredens 2012).

There is, again, considerable national variation in the role of teachers in guiding young people in internet safety (Figure 2).

Teachers in the United Kingdom are the most active in terms of giving internet safety advice (83%) and overall, teachers in Northern European countries adopted high levels of active mediation of children’s internet use. By contrast, some Southern European countries (Italy, Greece) and countries in the East (Romania) had less. The range of variation is considerable: from 93% of teachers
QC338: Have any teachers at your school ever done any of these things? (Multiple responses allowed)

Base: All children who use the internet.

in Norway to 56% of teachers in Italy practicing at least one form of internet safety (Livingstone, et al. 2011).

The European Commission’s Education, Audiovisual and Culture Executive Agency (EACEA) also found wide variation in the availability of internet safety within school curricula (Eurydice 2009). Of 30 countries studied, 11 did not have any provision for the subject. Of the 15 countries that had introduced internet safety, most had done so relatively recently (70% had introduced the subject since 2006/7), mostly at secondary level and not always consistently (European Commission 2009: 17). Online safety was not available in the school curriculum in Sweden, Belgium (German-speaking community), Denmark, Italy,
Iceland, the Netherlands, Bulgaria, Greece and Hungary. As of 2009, plans were underway to introduce it as a formal element in Belgium, Greece, Romania and Iceland. In some countries (Bulgaria, Germany, Cyprus, Lithuania, Austria and Slovenia), online safety was taught only at secondary level. At the primary level, internet safety was more likely to be treated on a more informal basis as part of specific educational projects or as part of other subjects whereas at secondary level a more structured approach tended to be adopted within ICT-related or media education courses.

The Message of Internet Safety
Not only is there wide variation in the provision of online safety education, there is also considerable diversity in what it contains. Efforts have been made by a number of international agencies to bring some consensus to the range of issues taught. UNESCO’s ICT Competency Framework for Teachers (2011), for instance, recommends a comprehensive treatment of the following within teacher-training programmes to ensure that teachers are able to identify and manage internet safety issues such as:

- cyber bullying
- appropriate information to post
- predators
- communication forums
- privacy and piracy issues
- viruses
- scams
- spam
- cookies
- pop-ups
- intellectual property rights
- copyright
- inappropriate content
- digital citizenship
- email etiquette
- ethics
- legal requirements
- confidentiality of personal data

Insafe, the European network of Safer Internet Centres, identifies an equivalent list of issues that teachers should be able to respond to:

- Blogs
- Chat-based services
- Child sexual abuse images
- Cyberbullying
- Filtering and monitoring
- Mobile phones
- Online gambling
- Online gaming
- Sexting
- Spam, phishing and pharming
- Viruses and malware

2
ENISA, the European Network and Information Security Agency, under its remit for promoting awareness of secure networked communications, has likewise identified core topics for education as a basis for children’s safe internet use. The focus of its resources for education include training materials on security in areas such:

- Cyber Bullying
- Online Grooming
- Children in virtual worlds
- Security issues in online social networking
- Cookies
- Secure printing

(ENISA 2012)

The Eurydice survey of online safety education within schools found some consistency in the 15 countries where formal curriculum provision for internet safety was reported (Table 1).

Table 1. Internet Safety Topics by Country (2007/2008)

<table>
<thead>
<tr>
<th></th>
<th>BE</th>
<th>BG</th>
<th>CZ</th>
<th>DE</th>
<th>EE</th>
<th>ES</th>
<th>FR</th>
<th>CY</th>
<th>LV</th>
<th>LT</th>
<th>MT</th>
<th>PL</th>
<th>SI</th>
<th>FI</th>
<th>UK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online safe behaviour</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Privacy issues</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Cyberbullying</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Download and copyright issues</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safe use of mobile phones</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contact with strangers</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other topics</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

Source: Eurydice 2009.

‘Online safe behaviour’ as an overarching theme was represented in all cases, focusing in particular on the risk of ‘online grooming’ and other forms of dangerous online contact. Under this heading, children are taught ‘not to reveal personal information, nor give out their address, name of their school, telephone numbers etc.’ (Eurydice 2009: 8-9). Similarly, ‘privacy issues’ teach students to control how much information they reveal about themselves on social networking sites and blogs. At a more advanced level, students may learn about how companies gather data on individuals and use it for commercial and other purposes. Relatedly, ‘contact with strangers’ is also widely represented
as a topic, warning students about risky forms of contact. ‘Downloading and copyright issues’ was another aspect of internet safety education found in all cases, teaching students about copyright in online materials and the risks of illegal file sharing. Two topics, closely related to peer cultures among young people, namely cyberbullying and the safe use of mobile phones, were not as widely found within internet safety classes but, the report notes, were frequently included as part of special programmes within schools. Additionally, topics such as dealing with computer viruses, security issues, legal aspects and online commercial risks were also listed as part of school curricula on internet safety.

There would appear to be a general consensus, therefore, about the kinds of risks that need to be highlighted in internet safety education. Predominantly, these refer to protection of personal information (communication risks) and threats from strangers in online situations (contact risks). The teaching of internet safety, as such, emphasises a protectionist approach urging young people to be cautious with disclosure of personal information, to be careful in new situations, repeating the age-old adage of not talking to strangers, and in general adopting a protectionist stance towards issues of personal safety and security. It also reflects to some extent the sensitivity within schools about security of information systems and the need to protect the school IT infrastructure from viruses or harmful use. This is reflected in the importance for many schools of a robust Acceptable Use Policy (AUP) governing access to its IT systems, supported in many instances by filters which control access to content deemed by the school to be unsuitable.

How are such risks identified? Ideally, online safety education, just like the policy agenda itself, should be evidence-based and, at the least, evidence-informed. Yet, empirical evidence, particularly at the European level, has until relatively recently been quite sparse. As such, the early history of internet safety messaging was more likely to have been crafted in response to risks perceived by policy makers and by child welfare groups to be particularly pernicious, or by pressure from the general public, often in the form of a media-inspired, moral panic prompted by sensational events. As research develops and understanding of the nature of risks has improved, the potential of a disconnect increases between internet safety as taught and the reality as revealed in research or as experienced by young people.

Reporting on the available evidence in 2009, EU Kids Online identified a ranking of the top five risks cited within some 400 research studies in Europe (Livingstone and Haddon 2009):

- *Giving out personal information* was the most common risky behaviour affecting around half of all teenagers online;
- *Seeing pornography online* was the second most common risk at around 4 in 10 teenagers across Europe;
• *Seeing violent or hateful content* was the third most common risk, experienced by approximately one third of teenagers;

• *Being bullied online* (cyberbullying) came fourth, affecting some 1 in 5 or 6 teenagers online, along with receiving unwanted sexual comments – experienced by between 1 in 10 teenagers (Germany, Ireland, Portugal) and as many as 1 in 3 or 4 teenagers in Iceland, Norway, UK and Sweden, even rising to 1 in 2 in Poland.

• Last, *meeting an online contact offline* was the least common though reputedly the most dangerous risk.

Therefore, the degree of emphasis given to risks such as online grooming in online safety education in contrast to more conduct-related risks such as cyberbullying is hard to understand. While extreme but rare cases of grooming cause much public anxiety, the overly protectionist approach reflected in much school-based safety advice may have the effect of accentuating the gap many young people may feel between their online experiences in their own lives and that encountered within the school system. This was noted also in the Eurydice assessment of internet safety education (2009) which questioned the practice in many schools of banning applications such as social networking sites on their systems, missing out on valuable opportunities to learn responsible behaviour in some of the most popular applications on the internet (ENISA 2012). In this way, educationalists may find that their interventions are ineffective when, in the context of highly regulated schools’ information systems, they seek to protect young people from dangers and risks they experience as commonplace in their daily lives.

**The Effectiveness of Internet Safety Education**

The effectiveness of overly-protectionist approaches towards internet safety education is increasingly questioned by researchers (Jones 2010, Jones and Finkelhor 2011). Successful examples of public safety promotion (anti-smoking campaigns, wearing a bicycle helmet, use of seat belts in cars, for example) may provide, it is argued, useful models of how to effect change in online behaviour. According to Finkekhor et al., effective programmes tend to work because of their specific and targeted nature and the fact that there is a high degree of consensus about the connection to harm (Finkelhor, Wolak, and Mitchell 2010). Internet safety messages, such as ‘never give out personal information’, or ‘don’t talk to strangers online’, by contrast, lack this clarity. There are situations where giving out personal information may be a good thing, just as talking to strangers is taken for granted as being part of youthful online social interaction.
In practice, providing online safety advice about communicating with strangers or information disclosure is something that needs to be tailored to the specific context, and especially according to the age of the user, the primary basis on which young people’s online practices are differentiated. More complicated still are questions related to potentially harmful content such as pornographic sites and the sending of sexual messages, around which there will be more complex moral concerns as well as cultural variation, leading many teachers and schools to avoid the topic altogether. Accordingly, internet safety education needs to be contextualized to a much greater extent, disseminated cautiously and located within evidence-based analysis of real world accounts of youthful experiences (Finkelhor, et al. 2010). So, for example, the topic of appropriate privacy settings on social networking sites is a topic that research identifies as an important risk for many young people (Lenhart, et al. 2007; Staksrud 2008).

Extensive educational efforts in the United Kingdom and Ireland targeted at changing young people’s behaviour in personal information disclosure appear to have paid off with marked changes in the numbers of young people who keep their social networking profiles private (Grehan, McLaughlin and O’Neill 2012). However, much greater evaluation is needed about what works and what doesn’t in educational settings. In many cases, little or no evaluation takes place and there is very little evidence of the impact that education has had on young people’s approaches to safety or attitudes to risk. The absence of research is likely to mean that policy is driven by anxiety rather than knowledge and that educational responses will be ineffective and poorly targeted (Finkelhor, et al. 2010). Rather, a focus on real as opposed to perceived harm, and identification of the problematic behaviours that education seeks to target, is likely to be more effective. In relation to ‘sexting’ for example, Finkelhor et al (2010) argue too vague a definition will serve as a barrier to the provision of effective education or safety messaging. Instead of the imprecise and sometimes misleading media reporting of sexting as a phenomenon (Sacco 2010), evidence of where real harm is likely needs to be identified and highlighted (e.g. situations where adults use the internet to induce youth to send sexually explicit images of themselves, or where peers use images to blackmail or humiliate others).

The analytical distinction between risk (the probability of harm) and actual harm is, therefore, vital for improving educational effectiveness of internet safety programmes (Jones and Finkelhor 2011; Livingstone, Haddon and Görzig 2012). Risks do not inevitably result in harm, nor are they inherently bad (Livingstone, this volume). Yet, more often than not, it is the risk rather than the harm that is the focus of safety education. So, for example, meeting new people online is a common type of risky behaviour engaged in by young people (Livingstone, et al. 2011), rarely resulting in harm. Focusing exclusively on the risk by seeking to ensure such meetings never happen is likely to be ineffective while identifying those factors that are more likely to lead to harm
may prove a better strategy. The elimination of risk, likewise, may not always be in the best interests of children. Arguably, risks are an important part of the developmental process of growing up and the experiencing of risk is essential to building resilience (Livingstone 2010). It is those who are especially vulnerable – those who have psychological difficulties, are socially excluded (ostracised), engage in unhealthy sensation seeking behaviours or are in some way or another members of a vulnerable group (Görzig 2011) – that need to be specifically targeted to make educational interventions more effective. Such children may lack effective parental support making the input of teachers all the more important. Moreover, with the age of first internet use ever decreasing, schools need to develop new ways of reaching younger children providing age-appropriate training and advice. In-service training may be required to equip teachers, particularly within the primary sector where ICT use is relatively new, with the skills to support younger children. Importantly, children’s own skills need to be emphasized to include decision-making skills that improve safety as well as creative, critical and productive skills that enhance children’s digital literacy. Such assistance may take the form of more generic skills to improve young people’s decision-making, health and safety across a wide range of situations, both online and offline, for example, in risk assessment, emotion management, perspective-taking and help-seeking (Finkelhor 2011). This remains an ambitious objective for education, particularly in the context of the many competing demands for curriculum attention. The extent to which such objectives can be incorporated within the broader agenda of digital literacy is considered next.

**From Internet Safety to Digital Literacy**

Our students have changed radically. Today’s students are no longer the people our educational system was designed to teach. (Prensky 2001)

Coinciding with calls on schools to include internet safety in the curriculum, education is also called upon to support wider ICT adoption through the teaching of digital literacy skills. Digital literacy is a complex and multifaceted concept, taken to include the many forms of engagement and articulation with digital technologies as they mediate most of our social interactions (Erstad, Sefton-Green and Nixon 2009). Associated both with technical skills or competence, as well as cognitive and critical abilities to use technologies for information retrieval and processing, digital literacy by virtue of its importance for governments’ strategies to build knowledge-based economies is now a high priority for educational systems (Cartelli 2012). Digital competence – the ‘confident and critical use of information society technology (IST) for work,
leisure, learning and communication’ – is recognized by the European Union as one of eight key competences for lifelong learning, essential for all individuals in a knowledge-based society (Council of the European Union 2006). Digital competence is also fundamental to the Digital Agenda for Europe and a key indicator for marking progress towards attainment of its goals (European Commission 2011). Encompassing the full spectrum of user skills from retrieval, access and exchange of information to communicating online, digital literacy, along with related concepts of media and information literacy, has come to occupy a central role in policy thinking about effective participation in information societies (Cartelli 2013).

In more exaggerated versions, such as Prensky’s ‘digital natives’ hypothesis (2001) quoted above, it is claimed that digital technologies change all aspects of education and bring about a completely new learning paradigm. More moderate versions imply more incremental change: students want technology to improve teaching and learning, but not to change it radically (OECD 2012). From the point of view of internet safety, digital literacy implies that young people need not just basic tenets of how to keep safe online, they also need a range of technical, cognitive and critical skills that enable them to make assessments about the quality of online sources, to use internet technologies wisely and creatively, and to gain competence in the use of digital tools for public participation.

Digital literacy and related concepts of media literacy, e-skills and digital competence (Ala-Mutka, et al. 2008; Lankshear and Knobel 2008) typically focus on a mix of skills, knowledge and attitudes that individuals require in the course of their everyday interactions with digital technologies. Gilster (1997), credited with coining the term, characterized digital literacy as the new set of challenges that arise in understanding and using information accessed through digital networks. Later versions have sought to characterize the developmental steps associated with the acquisition of digital literacy. The DigEULit project (Figure 1) identifies three levels or stages for digital literacy development.

**Figure 3. Levels of Digital Literacy**

<table>
<thead>
<tr>
<th>Level I: Digital Competence</th>
<th>Level II: Digital Usage</th>
<th>Level III: Digital Transformation</th>
</tr>
</thead>
<tbody>
<tr>
<td>(skills, concepts, approaches, attitudes, etc.)</td>
<td>(professional/discipline application)</td>
<td>(innovation/creativity)</td>
</tr>
</tbody>
</table>

At its foundation, are the skills and competences, including basic technical skills as well as multifunctional competences that can be applied in different contexts (Level 1). These underpin digital usage (Level 2) in which users draw upon relevant digital competences within particular personal and professional contexts. Level 3 is a point of digital transformation where digital usage is internalized and stimulates innovation and creativity through being fully incorporated into the relevant domain.

It is interesting to look at this framework for the development of digital literacy alongside actual patterns of young people’s internet activities and skills. Findings from EU Kids Online (Livingstone, et al. 2011) point to a ‘ladder of opportunities’ whereby basic activities tend to be done first by most children (Livingstone and Helsper 2007). When children start to use the internet, among the first things they do are schoolwork and playing games. EU Kids Online found that nearly 14% of European children on average do not get further than this. Next, children start to use the internet as a medium of entertainment, for instance, watching video clips. This progresses to interactive, communications-related activities and social networking. More demanding, creative and participatory activities come last and are undertaken by fewer children. Less than one fifth of 9-12 year olds and only a third of 15-16 year olds were found to reach this step.

Activities are also positively correlated with digital skills: the more children do online, the more skills they have (Sonck 2011). This has important implications for education in that encouraging young people to do more online is a good way of improving their digital skills. The safety skills asked about in the EU Kids Online survey included a combination of basic or functional skills (how to ‘bookmark a website’, ‘change privacy settings’, ‘block messages from someone you don’t want to hear from’) as well as informational and evaluative skills (how to ‘find information on safety’, ‘compare different websites to see if information is true’). An important finding is that these various skills go hand in hand and that those who practice good safety skills also have better informational skills (Sonck 2011). Therefore, the teaching of safety skills can provide a good basis for other digital skills.

Locating internet safety within frameworks for ICT education in schools is an important issue for consideration. Digital literacy, as we have seen, encompasses overlapping skills and knowledge domains including internet, media and information literacy aspects (Ala-Mutka 2011). Safety skills also represent increasing orders of complexity from basic instrumental and operational skills, through advanced competence and knowledge to attitudinal dispositions. From an instrumental point of view, young people need the skills to use browser software effectively and safely, to manage their personal profile information through the appropriate privacy settings, and to use safety features provided in software applications. As such, implementing safety draws equally on skills,
knowledge and attitudinal dimensions. At a more sophisticated level, children need not just operational skills but critical understanding of the capabilities, limitations and risks associated with different media, and the ability to process and form judgements on knowledge received through different channels. Then, at an attitudinal level, students need to acquire and internalize an understanding of safety in the context of all their online interactions, developing an attitude of responsibility towards safe and productive participation in the digital environment. This encompasses not just a critical attitude towards contacts and content encountered online but also an ethical and critical understanding of one's own activities, reflecting on the consequences of accessing content, creating and uploading material and behaving and communicating with others (Ala-Mutka 2011: 52).

Taken together, this broad set of educational objectives – more widely known as digital citizenship – envisages the school setting as the environment best suited towards fostering the diverse cognitive and perspective-taking skills increasingly required in mediated societies (Mossberger, Tolbert and McNeal 2008; Tynes, 2007). School systems have responded in a variety of ways to the challenge of digital literacy and ICT education (Ferrari 2012; OECD 2012; Redecker, et al. 2011). Given its dynamic and changing nature, educational planners have tended to incorporate digital literacy skills across the curriculum rather than within a single subject and to use the idea of an ICT framework – a structured set of intertwined competences – to act as a guide for curriculum organization. The ICT Framework for schools in Ireland (NCCA 2007), for example, encourages teachers to embed ICT as a cross-curricular component for all subjects. Aiming towards progressive attainment of skills from the early years of secondary schooling, it envisages multi-layered skills, attitudes and knowledge associated with:

- the potential of ICT to create, communicate, and collaborate to organise and produce information;
- understanding and applying knowledge of the functions of ICT including safe practice, maintenance and ergonomics;
- using ICT for critical thinking and learning including managing enquiry, assessing information, solving problems, and expressing ideas across a range of curriculum areas;
- developing a critical appreciation of the role of ICT in society and habits which reflect ethical and responsible use of ICT.

Skills and competences associated with individual media or technologies (the first levels of learning) thereby act as a foundation for higher level digital competence, emphasizing cognitive, critical, and ethical dimensions of practice and use. As such, digital literacy is proposed not as a subject in its own right;
rather, it is a framework that allows the translation of digital competence into educational programmes, and to act as a basis for the generic skills identified as important for lifelong learning (Ferrari 2012).

Given the importance of ICT development for governments, it is hardly surprising that education initiatives dedicated to digital competence have the priority they do. The OECD Programme for International Student Assessment (PISA) now recognizes problem-solving in a digital context and includes students’ ability to read, understand and apply digital texts in its assessment of student performance (OECD 2009). UNESCO, a longtime leader in promoting the concept of media education (Pavlč 1987; UNESCO 1982), has also promoted the concept of media and information literacy (UNESCO 2011a), supported by indicators that evaluate how societies respond in bringing about greater digital literacy (UNESCO 2011b). Interestingly, these assess both the availability of institutions that nurture and promote media and information literacy in society, as well as supports for teachers and teacher-training. Given repeated concerns that without adequate in-service teacher training, this is an important emphasis, without which the education system simply will not be able to respond to the many demands placed upon it.

Conclusion

With the teaching of internet safety now constituting a cornerstone of European strategy for a better internet for children (European Commission 2012), schools that may in the past have found themselves ill-prepared for the wider deployment of ICT across the curriculum, now face new responsibilities and challenges at the forefront of international efforts to enhance safety and digital literacy skills. Many educational systems have introduced internet safety in their curricula; some as a specific subject or special project, others by incorporating it within relevant curriculum areas such as social and personal health education, or civic and political education. Whichever method is adopted, educational systems and more specifically schools have assumed a more prominent role than heretofore in ensuring that students learn appropriate behaviours on the internet, safety instructions as well as coping mechanisms in the cases where upset or distress occurs. Worryingly, the technology gap between students and teachers, and the disconnect between digital literacy within and beyond school, may undermine the effectiveness of such efforts (Burnett 2011; Meneses, Fabregues, Rodriguez-Gomez and Ion 2012; Moursund and Bielefeldt 1999). The issue of internet safety in education and especially for policy making is therefore twofold and requires policy to support the training of teachers as well as the education of students.

Two main strategies towards internet safety education have been identified in this chapter: one targeted and subject-specific, and the other a longer term
curricular movement towards digital literacy education. The first trajectory provides a contingent response to the many urgent calls for action by policymakers and child safety experts in helping children and young people deal with risks in the digital age. Researchers have urged caution about the degree of emphasis on such programmes given the general nature of the objectives of internet safety and the likelihood of resistance to messages that are overly-protectionist and which do not speak to the realities of young people’s digital experience. The second approach, which seeks to develop children’s online safety skills within the context of an expanded concept of literacy and digital citizenship, marks a shift towards empowerment and greater self-regulation by young people. This, as we have seen, while arguably the more sustainable approach that best meets young people’s needs, poses substantial challenges for schools and for governments resourcing them. Yet, as international pressures mount between countries in pursuit of competitive advantage in digital literacy attainment, this may represent an important opportunity to seek a secure and widely accessible position for internet safety education.

Notes
1. The Education, Audiovisual and Culture Executive Agency (EACEA) is responsible for the management of certain parts of the EU’s programmes in the fields of education, culture and audiovisual. The Eurydice Network provides information on and analyses of European education systems and policies. See: http://eacea.ec.europa.eu/education/eurydice/index_en.php

References


UNESCO (2011a) *Fez Declaration on Media and Information Literacy.* Paris: UNESCO.


Chapter 11

Parents

Mediation, Self-regulation and Co-regulation

Giovanna Mascheroni, Maria Francesca Murru, Elena Aristodemou & Yiannis Laouris

The prominent role of parents in regulating the risks and benefits of the internet for children is becoming more and more valued within public and policy debate. Two parallel processes that involve both public and private dimensions trigger its increasing relevance. On the one hand, the recent emphasis on empowerment as the preferred regulatory approach in the field of children's media consumption (Oswell 2008), together with the increasing complexity and fragmentation of the media environment, have suggested the delegation of regulatory authority to families. Parents are no longer viewed as passive media users that need to be guided and protected in their media consumption. Rather, as media-literate users, they are expected to protect themselves and their families from potentially harmful content (Helberger 2008; O'Neill 2008). On the other hand, home has become the most common location for internet use (Livingstone, et al. 2011); thus, the responsibility of guiding children's online behaviour lies most appropriately with parents, who are closest to children and best positioned to give them the guidance they need.

However, this increasing relevance of parental mediation is paradoxically counterbalanced by a variety of structural conditions that complicate and partially hinder caregivers’ support. Internet risks are much more varied and potentially dangerous than those posed by the broadcast media which are characterised by an institutional separation of production and reception and, therefore, by a highly controlled top-down flow of communication. At the same time, online opportunities cannot be ignored. Digital and online media – embedded almost everywhere in social life – offer unprecedented opportunities in the field of relationships, identity, self-actualization and education. As a result, they are crucial factors in socio-cultural inclusion (Livingstone and Helsper 2007), and, therefore, any action that limits or constrains children's online opportunities needs to be carefully considered.

Moreover, the design of online devices and environments, as well as their associated frames of use, make it difficult to apply traditional parental media-
Monitoring strategies that regulated children’s relationship with broadcast media such as the unobtrusive ‘cursory glance from a distance’ are undermined by the multitasking practices of internet use. General trends of privatisation, e.g. small-sized screens that discourage shared activities, as well as segmentation of media consumption within homes (Livingstone 2002), further undermine the effectiveness of parental supervision. Thus, while safety policies are increasingly relying on the presumed advantages of parental mediation, the role of family negotiation in framing young people’s access to the internet is taking shape within a material and cultural environment that combines unprecedented responsibilities and challenging hindrances.

This chapter aims at tackling that apparent paradox by proposing a two-step research approach. First, drawing on data from EU Kids Online, we investigate practices of parental mediation in order to assess their efficacy. In light of these findings, we then present and discuss new ways of connecting policymaking and parental mediation. We argue that the composite and precarious balance implied by processes of parental mediation require alternative frames of policymaking within which parents as the principal stakeholders together with children can play a crucial role. Finally, we examine the expediency of the active involvement of parents in online safety policy, not only as targets of safer internet messages but also as co-developers of goals and strategies.

Parental Mediation: Practices and Effectiveness

Parental mediation of children’s internet use involves the management of the relationship between children and media by their parents, including those strategies aimed at minimising online risks and maximising the benefits of online activities. Drawing on prior literature on parental regulation of children’s television viewing (Valkenburg, et al. 1999), as well as introducing new typologies for internet-specific activities, four main categories of parental mediation are proposed:

1) ‘social mediation’ combines activities derived from television viewing (Livingstone and Helsper 2008), namely active mediation and co-use, including talking about media content while the child is engaging with it, and sharing the online experience of the child by remaining nearby;

2) ‘restrictive mediation’ involves setting rules that limit and regulate time spent online, location of use, and content;

3) ‘technical restriction’ is the use of software and technical tools to filter, restrict and monitor children’s online activities; and finally,

4) ‘monitoring’ or checking up on children’s online practices after use (Livingstone and Helsper 2008).
The EU Kids Online survey asked parents which mediation strategies they practiced, while also asking children which mediation activities their parents engaged in. The distinction is made here between active mediation of internet use more generally (where the parent is present or nearby, discussing or sharing internet activities) and, in particular, the active mediation of internet safety (where the parent actively guides the child to use the internet safely).

**Figure 1. Parental Mediation According to Children and Parents**

Positive support of children’s internet use, safety guidance and setting rules to regulate use are the most popular strategies adopted by European parents: according to children, 87% of parents engage in one or more forms of active mediation of internet use (talk to their children about what they do on the internet, stay nearby, encourage the take up of opportunities, sit together or share activities online); 86% actively mediate internet safety (suggesting how to use the internet safely and ways to behave with other people online, giving support when the child is bothered by risky online contact, conduct or content); and 85% practice one or more forms of restrictive mediation (setting bans on specific activities such as having a profile on a social networking site, using instant messaging, uploading photos or video, and downloading music or films, or preventing children from giving out personal information online). Monitoring internet use (checking which websites the child has visited, checking his/her profile on social networking sites and his/her list of contacts, checking the content of email or IM messages) is relatively low in comparison to other forms of parental mediation and is adopted by only one in two parents. The use of technical tools to filter and keep track of children’s online activities is the least favoured mediation strategy: the major form of technical intervention is the use of software to prevent spam and viruses, adopted by nearly three
quarters of parents; around a quarter of households use parental controls to block content or to track the websites visited by their children, while only a minority use services that limit time spent online.

Findings reveal substantial age differences in the different kinds of mediation considered: active, restrictive, technical mediation and monitoring, all show a substantial decline as children grow older. Gender differences are less notable, though girls tend to receive a little more support regarding interactions or content that has bothered them online, and tend to be a little more restricted than boys.

With regard to cross-national comparisons, country differences between active mediation of internet use and the mediation of internet safety are small, perhaps due to the social desirability of active mediation compared to other regulation strategies. Findings show, instead, a considerable variation by country in the use of restrictive measures such as the use of filtering technologies and monitoring.

Besides country variations, a further issue is the potential discrepancy in reports of mediation by parents and by children. Previous research (Livingstone and Bober 2006) has revealed a considerable generation gap, with parents reporting more mediating activities than are recognised by their children. By contrast, the EU Kids Online findings signal a higher level of agreement between parents and children in each of the areas of active mediation, safety guidance, restriction, monitoring and the use of filtering tools (see Figure 1). When looked at on a cross-national basis, however, there are higher degrees of disagreement between children and their parents in some countries for specific mediating activities: children and parents disagree slightly more in Sweden and Finland, and Sweden and Germany with regard to active parental mediation and safety guidance respectively; disagreement on restrictive measures is higher in Poland and Estonia, while it is more substantial in Finland, Denmark and Norway on the use of monitoring; finally, disagreement on technical mediation is common in a variety of countries.

Earlier research (Livingstone and Helsper 2008; Kirwil, et al. 2009) has also investigated the potential effects of parental mediation on children’s use of the internet, examining particularly whether it is associated with a reduction in children’s exposure to online risks. Studies are inconclusive, claiming variously that restrictive measures or, at the opposite end of the spectrum, active mediation of use are effective.

In order to investigate the relationship between mediation and online opportunities and risks as experienced by children, a correlation was conducted between demographic variables (age and gender of the child), mediating strategies (active mediation of use, active mediation of safety and restrictive rules), children’s exposure to online risks, level of harm experienced, digital skills and number of online activities as an indicator of online opportunities. As most parents tend to overestimate their mediating activities for reasons of social desirability (Fujioka and Austin 2002; Livingstone and Helsper 2008),
the mediation indices are based on children’s reports. We must also recognize that the distinction between various strategies is analytical in nature, and that parents in practice tend to combine diverse activities: therefore, measuring the impact of each mediating activity in isolation is difficult.

Findings confirm that age is negatively correlated with active mediation \((r=-.23)\), safety guidance \((r=-.14)\) and restriction \((r=-.50)\), signalling that parents tend to reduce their intervention as children grow up. Findings also show statistically significant correlations between mediation and risk exposure, digital skills and online opportunities. Restrictive mediation by parents has the highest negative relation with the experience of risks \((r=-.36)\), online opportunities \((r=-.52)\) and internet competences \((r=-.39)\), indicating that restrictive rules can reduce exposure to the risks of the internet while at the same time restricting its beneficial outcomes and the level of digital literacy. The impact of active mediation of internet use and active mediation of internet safety on risks is lower \((r=-.12\) and \(r=-.03\) respectively; while active mediation of use is also negatively associated with opportunities \((r=-.05)\) and online skills \((=-.03)\), the correlation between safety guidance and opportunities and skills is positive \((r=.04\) and \(r=.03\) respectively).

The same relations are represented graphically in Figure 2. This shows that only restrictive mediation leads to a smaller number of children who have experienced at least one of the seven risks measured. If we look, instead, at parental mediation as reported by parents, children’s exposure to online risks decreases the more parents adopt restrictive measures and actively mediate their children’s internet use; conversely, parental active mediation of safety has no significant association with online risks for children aged 11-12 but it is associated with more risks for 9-10 and 13-16 year olds (Dürager and Livingstone 2012).

**Figure 2.** Parental Mediation and Children’s Risk Exposure on the Internet

<table>
<thead>
<tr>
<th>% children have experienced any of the 7 risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active mediation internet use</td>
</tr>
<tr>
<td>Yes</td>
</tr>
</tbody>
</table>

Base: all children aged 9-16 who use the internet.
Risks, however, do not necessarily involve harmful consequences (Livingstone, et al. 2011). When examining the relationship between mediation and harm (Figure 3), findings may at first sight seem counterintuitive: it would appear that both active mediation of internet use and internet safety lead to higher levels of harm. However, this may in fact work in reverse: children who have had a negative experience online receive greater attention by their parents as they may be more concerned for their online safety. In line with the analysis of risks, only in the case of restrictive mediation do children report a substantially lower incidence of online harm.

Figure 3. Parental Mediation and Children Being Harmed Online

According to children’s reports about their parents’ online mediation, only restrictive strategies, therefore, prove effective in reducing risks and harm experienced by children. If we consider, by contrast, parents’ accounts, parental restrictive mediation leads to a significantly smaller probability of being bothered or upset online at any age, while active mediation of internet use tends to decrease the experience of harm by children aged between 9 and 12 years (Duerager and Livingstone 2012). At the same time, a significant proportion of children report ignoring totally (7%) or to some extent (29%) what their parents say about the internet, thereby limiting its effectiveness. Nearly one third (30%) claim parental mediation is not helpful.

The strong correlation between risks and opportunities (Livingstone and Helsper 2007 and 2009, Livingstone, et al. 2011) also has to be taken into consideration when assessing the role of parental mediation. More specifically, restrictive mediation is likely to restrict opportunities and the development of digital literacy while reducing the number of risks children encounter online. Figures 3 and 4 show how those children who are restricted by their parents in
terms of time spent online, or in the online activities they are allowed to engage in, benefit from fewer opportunities and are less skilled than children who are not subject to restrictive mediation. On the contrary, children whose parents actively mediate their internet use or internet safety report more skills (around one skill more out of the 8 surveyed) than children of non-active parents. In the case of online opportunities, the difference between children who report active mediation and those who do not is less significant.

**Figure 4. Parental Mediation and Online Opportunities**

![Parental Mediation and Online Opportunities Graph](image)

Base: all children aged 9-16 who use the internet

**Figure 5. Parental Mediation and Digital Skills**

![Parental Mediation and Digital Skills Graph](image)

Base: all children aged 11-16 who use the internet.

Furthermore, a model by Kirwil and Laouris (2012) to assess how much experimenting with self-presentation online matters as a predictor of undertaking
risky activities online has shown that it explains most of the variance. This again points towards restricting children’s time alone in front of computers. Contrary to the hopes of policymakers and parents, except for restrictive measures and active mediation of internet use, introducing forms of parental mediation is unlikely to actually reduce the supposed harmful consequences of certain online activities. In addition, initiatives that are more effective in preventing children from exposure to risks, such as setting rules for internet use, have the side effect of reducing both online opportunities and digital skills, which in turn may help children cope with internet risks and harm. Therefore, awareness campaigns tend to emphasise parents’ engagement in children’s online activities rather than, or in combination with, restrictive regulation.

Parental Mediation in the Family System

These apparently discomforting findings do not necessarily warrant a dismissal of parental mediation as a key element in internet safety policy. Rather, they suggest the necessity of rethinking parental mediation as it has been integrated within policy frameworks and of the ways in which its implementation has been conceived and planned.

First of all, the tightly-woven social fabric in which parental mediation occurs needs to be recognized. Rather than a neutral channel through which safety awareness can flow, it might be more useful to view it as a delicate balance of different social and cultural elements that take shape within families. To date, thinking about parental mediation has focused more on the strategic dimensions of parents’ management of the relationship between media and their children. However, the lived experience of media use within families suggests a more complex situation.

Parental mediation is not only the intentional effort on the part of parents to maximize the benefits and minimize the risks of media and internet use on children’s wellbeing. It is a contingent outcome of changing balances in relationship, identities and values within the family system. This is broadly consistent with the theorization of parental mediation as one of the ways in which the family reproduces its values in the face of external meaning systems (Warren 2005; Livingstone 2002). Media, of course, are not the only subject of disciplinary rules imposed by parents in order to prevent unwanted influences. They do, however, constitute resources of meanings that families actively incorporate in confirming their hierarchy of values and reinforcing familial ties. Against this background of values and signification, researchers have identified two main elements as particularly relevant to parental mediation: family communication patterns and parenting styles.
Nathanson (2001) has identified two main attitudes in families’ communication patterns: a “socio-oriented” attitude where general harmony is encouraged and controversial stances are avoided, and a “concept-oriented” approach where free and independent reasoning is valued regardless of its consequences on general agreement. Four ideal-types of communication pattern arise from the intersection of these two main attitudes; they function as cultural and cognitive frames for media consumption and media governance within the family’s system. A predominance of a concept-oriented attitude will lead towards a pluralistic environment, celebrating media diversity; on the other hand, a socio-oriented attitude is one that supports a more protectionist communicative environment. Where neither a concept-oriented nor a socio-orientation is evident, a “laissez-faire” style results and media will rarely feature in the family system and parental management of children’s access to media will be soft and almost invisible. Finally, the convergence of a concept and socio-orientation will result in a “consensual” family model, where media practices are discussed and shared within a constant exchange of ideas and suggestions.

Research by Eastin et al. (2006) found that parenting style has a significant effect on all forms of mediation of online content. Among the four types of parenting studied – authoritative, authoritarian, permissive, and neglectful – it is authoritative parents, who are most likely to be committed to mediation of children’s internet usage and to be more responsive and stricter than average. Authoritative parents, in this context, ‘monitor and impart clear standards for their children’s conduct’ (p. 487); they are assertive and supportive, and want their children to be socially responsible and self-regulating. Authoritative parenting is characterized by high levels of demand, warmth and psychological autonomy. Such parents tend to adopt a wide array of strategies, including restrictive techniques but complemented by shared usage as well as mutual exchange of support and advice. Authoritarian parenting, by contrast, is characterised by obedience-oriented rules and high levels of behavioural control, as for instance by the use of technological blocking. Permissive parenting makes few demands on children, allowing children to regulate their own behaviour without confrontation. Finally, uninvolved or neglectful parents are defined as low in responsiveness and in the demands on children.

Faced with such diverse values and attitudes, the real challenge for policymakers is thus taking into account all the deep and irreducible differences that characterize parental mediation. Historically, the delegation of responsibilities to parents has involved the definition of public criteria that tend to homogenise parental mediation and set standards of good parenting. However, this homogenisation contrasts with the variety of parental practices and values highlighted by research. As Oswell argues, “any devolution of authority (in the context of moral, religious, and cultural value) is matched by a continuation
and accentuation of historic forms of normalization (mediated by scientific and professionalized expertise)” (2008: 479).

“Normalization” is not the only practicable route to ensuring online safety for children. Alternatively, parental involvement can also be strengthened through enhancing their role as carers through greater awareness and media literacy. The next section considers some of these alternative options and discusses their feasibility in the light of some concrete examples.

Parental Involvement: Opportunities and Limits

Stakeholders in the field of internet safety have long advocated that parents should spend more time with their children in internet-related activities. However, identifying where parental involvement is most needed remains a priority. A comprehensive study conducted by the Cyprus Neuroscience & Technology Institute (CNTI) for the project InetRisks in 2008-2010, revealed that interaction and involvement of parents with their children in their online activities is bi-directional and mutually beneficial. Specifically, the InetRisks project hypothesised that perceptions of online risks on the part of uninvolved parents might be misleading and pose a threat by itself. Therefore, the project examined parental perceptions both at the beginning of the intervention and at the end after exposing them to a series of online activities in which their children acted as mentors. The analysis revealed that parental perceptions of internet risks changed. Through co-use with their children, parents were able – after being exposed to those risks – to better understand the severity of online threats and to figure out how to best protect against them. On another level, parents expressed satisfaction that co-use offered them an opportunity to spend ‘quality time’ with their children, and enhanced their level of knowledge in relation to ‘teen matters’ and technology. As it happened, parents participating in this study were educators and the experience enabled them to identify ways through which they could better support their students and plan curricula for activities related to internet safety.

Research continues to stress the importance of educating parents about internet threats (Diamantouros, et al. 2008; Cho and Cheon 2005; InetRisks 2010) and equipping them with the appropriate tools to protect their children (Cho and Cheon 2005). Parental awareness has also been the focus of many awareness raising campaigns by Insafe and by Safer Internet Centres in Europe. However, as the InetRisks project reveals, this approach alone is not enough. If parents are unable to conceive the magnitude of those dangers, even in their lightest forms, then their approach to support and help their children will probably be inadequate. Participating parents also contributed to the design of safer internet campaigns in Cyprus, both for meeting their
own needs as parents and those of their children. This involvement resulted in the organization of conferences that focused on children and parents, the exchange and learning of experiences as well as the brainstorming of ideas. The outcomes so far, have been successful as parents feel more involved in their children’s lives, and children can once more feel closer to their parents on a friendship level. Helping parents understand all angles of internet safety diminishes their fears and limits their tendency to restrict their children’s access to the internet. As argued above, parental mediation requires regulation if it is to be effective. And who is more appropriate to set the rules than the parents themselves?

Another case study, an EU-funded project called Simsafety, examined parent-child behaviour and interactions in virtual environments where internet dangers were simulated. Simsafety is a 3D educational game that works much like Second Life™ in which students are engaged through constructivist/experiential learning models in coping with internet dangers. The virtual environment includes “buildings” where visitors can find information regarding internet safety, gaming areas where risks and dangers are simulated, a reporting area in which gamers are encouraged to report harassment, inappropriate behaviour or lost and found items. The whole environment provides a unique opportunity for a family game, through which children and parents can play and learn at the same time. Simsafety was piloted in various schools in Finland, Romania, Greece and Cyprus and the feedback from educators, parents and teachers was very encouraging. Parents emphasized the importance of having the dangers simulated in a controlled environment; it helped them appreciate and understand risks, rendering them more capable of guiding and consulting their children appropriately. Policies that encourage the development of products and which enable parents to spend quality time with their children constructively, contribute towards empowering caregivers’ ability to protect children in an era where technology is constantly changing and new dangers emerge.

The actual involvement of parents in policymaking, despite its potential advantages, remains very under-researched. A barrier to promoting their greater involvement remains the large percentage of parents in some countries that do not use the internet at all (Livingstone et al 2011). In countries such as Turkey, Cyprus, Greece, Romania, Portugal as well as Spain and France, more than twenty percent of parents of children, aged 9 – 16 years old, do not use the internet at all (Figure 6).

Digital literacy, it is clear, is a basic requirement to enable parents to protect their children online. Without knowledge of the online world or the activities their children engage in, it is practically impossible for parents to protect, advise or set rules about access and use of the internet. Given the pressures on families today, it is also difficult to get parents to learn about new technologies or to take on the heavy workload of digital literacy classes. Therefore, parental
involvement in children’s activities may prove to be a better solution towards targeting this problem. Parents who spend time with their children can learn how to use new technologies even at a basic level, while at the same time children gain the satisfaction of mentoring their parents. For once in their life, they get to teach, rather than be taught – itself a form of empowerment and responsibility. Adults, on the other hand, when encountering negative content can evaluate risks in a more critical and mature way and will be better able to advise and support their children. In addition, they can take advantage of the time they spend together with their children to transfer wisdom rather than technical skills. It is for this reason that the Insafe Network adopted this role-reversal strategy as the central theme of its 2012 Safer Internet Day international Campaign: “Connecting generations and educating each other”, with the slogan “Discover the digital world together...safely!”
Conclusion

Children access the internet mostly from home and therefore parents retain the major share of responsibility for protecting and regulating their children’s online access and use, especially when it comes to younger children. The benefits and importance of the role of parents in promoting children’s online safety is well established in research. Drawing on the findings of EU Kids Online, this chapter has explored the socio-cultural conditions and the variable degree of effectiveness of parental mediation. The low efficacy of parental strategies in reducing the supposed harmful consequences of certain online activities, together with the acknowledgment of a wide diversity in family values, attitudes and skills, suggest new ways of connecting internet safety policymaking with parental mediation. It is also vital that more is known about the impact of the generation gap in digital literacy between children and their parents in terms of how this affects parental mediation strategies and their varied efficacy.

The benefits of empowering parents and involving them more directly have been emphasised. Although parental awareness and involvement varies substantially across Europe (Eurobarometer 2008), the turn towards self-regulation and co-regulation both implies and relies upon parents as active, empowered and informed users. As such, parents are entitled to play their role in the shaping of policy. So, for example, parents might suggest that young children use the internet only in collaboration with them; at the same time, policy could focus on explaining and helping children understand why this is beneficial for them. Parents involved in policy making could also directly express their fears and concerns to policy makers and help them understand where weaknesses lie when it comes to protecting their children, so as to ensure such issues are covered in future campaigns.

Parental involvement in policy making is a matter of great importance and can be achieved through organized groups of parents that are willing to devote their time to this cause, as happens already in some European countries. Parents are at the base of the pyramid in the struggle to minimize children’s online risks and teach safer, more responsible behaviour when using the internet. Restricting or closing off internet use is not an option nowadays. With the rapid transition to a digital environment, new technologies offer great sources for education and countless benefits that enhance everyday life. Therefore, it is essential that policymakers target parents with programmes that help them understand the reasons why digital literacy is urgently needed, and encourage them to participate pro-actively in securing protection of their children and minimize the many risks that remain on the internet.
Notes
1. For example, the Audiovisual Media Service Directive (AVMSD) of the European Parliament (2007) advocates a new regulatory approach, which positions audiences as active, responsible actors able to exercise informed choices and protect their own interests. Self-regulation and co-regulation, in other words, presuppose a view of audiences as media-savvy.
3. See also Hasebrink et al. 2011.
4. This was the topic of the 2012 Safer Internet Day dedicated to “Connecting Generations, Discover the digital world together...safely!” aimed at encouraging parental active mediation of internet use such as engagement in forms of co-use.
5. For more information see the project’s website: http://www.simsafety.eu/. For the project’s deliverables and evaluation see http://www.simsafety.eu/index.php/library.

References


Chapter 12

Youth

*Revisiting Policy Dilemmas in Internet Safety in the Context of Children’s Rights*

Monica Barbovschi & Valentina Marinescu

Among the different myths that circulate within policy discussions of internet safety, two are especially prevalent. The myth of innocence (Meyer 2007) which promotes the image of the child-as-victim in need of adult supervision and regulation (Jenks 1996; Livingstone 2002), and its counterpart, the myth of the competent cyber-kid, both fail to capture the nuances of the various situations and roles children might find themselves in when using the internet. The first positions the child only in the role as passive recipient of content, without taking into consideration numerous contexts where children play an active role or may even initiate problematic conduct online (e.g. cyber-bullying). The latter does not take into account children’s incomplete social development and inability to assess complex social situations (including those online). The present chapter deals with the cleavage between the two approaches, namely the protectionist versus the participation approach, as articulated through various European policy documents and pits them against the data collected by the EU Kids Online II project (2009-2011) about children’s use of the internet and risks encountered online.

Children’s rights as detailed in the United Nations Convention on the Rights of the Child\(^1\) (UNCRC) provides a vital analytical lens with which to view these two contending approaches. The UNCRC established that children have a legal right to be protected from all forms of exploitation – including exploitation in cyberspace, just as it covers exploitation in the real world. Thus, articles 6, 12, 13, 16 and 17 of the Convention on the Rights of the Child could be assessed as setting up the general framework for regulating children’s online safety.\(^2\) At the same time, the Convention addresses the issue of parents’ responsibility for the upbringing of their children (Gjelsten, Simonnes and Kleven 2004) – likewise a responsibility that refers to both online and offline situations. At a global level the issue of children’s online safety remains regulated by the Convention and the “Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography”.\(^3\) At
the level of government, however, different frameworks for promoting a safer internet for children have evolved in the last two decades. Thus, in approaching protectionist vs. participation approaches in policy documents we restrict our analysis to the European Commission and the European Parliament legal acts that address the issue of children’s online safety and risks.

The chapter begins with a brief description of the two approaches in relation to the rights of the child, as stated by the UN Convention, and with a brief review of relevant notions of agency as contained in the new sociology of childhood (Jenks 1996, James and Prout 1997). Next, the chapter reviews the tension between protectionism versus empowerment as evidenced in the main guidelines of key European online safety policy, starting with 1996, but also including the Safer Internet Plus (2005-2008) and Safer Internet Programme (2009-2013). Furthermore, in light of the findings of the pan-European EU Kids Online survey, we discuss the appropriateness of the two approaches in relation to specific risks and in contexts of ‘digital agency’ practiced by children online.

**Children’s Rights in the Context of Internet Safety Policy**

Policy discourses on children’s use of the internet have struggled to balance protectionism with an approach that empowers children, or is participatory and child-inclusive. However, the dilemma of how much protection versus how much empowerment in specific instances, for specific age groups or specific internet risks is an ongoing one, kept alive by the discursive reproduction of media panics (Drotner 1999). As stated by O’Neill and McLaughlin (2010), protective measures directed at reducing risks might hinder access to various online opportunities. Therefore, solid evidence about risk and harm in particular is crucial in order to tailor protective/restrictive policy responses only when clearly needed, without undermining children’s rights.

The subjective and changing nature of notions of “good” versus “bad”, influenced by a variety of actors and factors, are constantly shaping policy measures. However, this normative distinction needs to be made explicit, as do the tensions that underlie it when it comes to deciding on imperatives in relation to children’s online activities.

The three P-s of the United Nations Convention on the Rights of the Child, namely Protection, Provision and Participation, are the three dimensions that encompass all the rights recognized in the Convention. The key elements of this legal framework can be found in article 12 of the Convention. As discussed in McLaughlin (Chapter 16, this volume), this article establishes the right of every child to freely express her or his views, in all matters affecting her or him, and the subsequent right for those views to be given due weight, according to the child’s age and maturity (Committee on the Rights of the Child 2009: 8).
This right imposes a clear legal obligation on States parties to recognize this right and ensure its implementation by listening to the views of the child and according them due weight. At the same time, expressing views is a choice for the child, not an obligation and states parties have to ensure that the child receives all necessary information and advice to make a decision in favour of her best interests (Committee on the Rights of the Child 2009: 8). The implementation of all other rights incorporated in the Convention is regulated in the body of the “General measures of implementation for the Convention on the Rights of the Child”. According to this article, a child holds rights which have an influence on her life, and not only rights derived from her vulnerability (protection) or dependency on adults (provision) (Committee on the Rights of the Child 2009: 8).

Participation rights have been considered the most controversial and difficult to implement (Handley 2005), and often in conflict with the competing rights to protection (Burr 2004). This dichotomy between rights, between welfare rights and self-determination rights, or protection rights versus participation rights, challenges the relationship between child and adult, as Wyness (2000: 6) accurately articulates. Whilst the view of ‘liberating’ children could be dangerous without balancing it with a protectionist approach (a view also endorsed by Lavalette in Qvortrup 2005: 163, where he speaks of the dangers of liberating the child from childhood), Wyness goes on to plead for education and policy initiatives that encourage more active participation of children. Moreover, while teenagers enjoy more agency than younger children, develop more elaborate identities and peer cultures, and challenge adult authority and conventions (Fine 2004; Coleman 2002), the latter have fewer opportunities to define their interests apart from those ascribed to them. On the moral grounds of ‘children’s best interests’, institutions and politicians had been taking decisions ignoring the voice of those they are supposedly protecting, rendering them ‘structurally invisible’ within the public sphere (Wyness 2000: 25). However, other theorists have contested the effectiveness of rights-oriented discourses and liberal approaches in advancing the well-being of children (Archard and Macleod 2002: 6), since different levels of cognitive comprehension are needed in order for children to gain information about their lives and their experiences, which would allow them to make informed decisions in their best interests.

Therefore, in order to transcend hidden normative, taken-for granted assumptions, a more ‘child-centred’ scientific approach is needed when dealing with the topic of children as victims versus children as competent agents. Research on children, as well as resulting policy responses, should, according to Livingstone (2002), emphasize the fact that children are to be seen as agents and not victims of internet-related practices.

Discourses about online risks posit children in a dualistic manner, both as objects of knowledge (what are the children doing or even worse, what are the
media doing to children?) and intervention (what can we do to minimize the risks that children face?) and as subjects of new competencies, which may or may not enable them to act in ways that minimize risks. In recent approaches to children and new media (Livingstone 2003; Byron 2008), the two sides do not always sit comfortably, and are often in conflict. While the former persists in the perception of children as vulnerable, objects of adult knowledge and intervention, the latter invites a more flexible approach.

The protectionist view of children has also been supported by large scale funding into research and intervention programmes designed to make the internet a safer environment for children. Before that, it was TV violence and violent video games that stirred up adult panics and invited protectionist interventions and regulations, ultimately denying children agency, as if they were helpless victims of the media (Buckingham 2000: 51). Thus, through wider access to the internet and new media, and easier availability of potentially detrimental influences and harmful impact, adult authority and a discourse of moral panic have been re-legitimized.

The position of moral rhetoric and depiction of children/teenagers as vulnerable, e.g. Brydolf’s (2007) positioning in terms of protection of the “inexperienced social networkers”, must be balanced with the view of children as skilled social agents – though in various degrees, as recent research suggests (Kuiper 2010: 8) – in asymmetrical power relations. Findings from EU Kids Online (Livingstone, et al. 2011) debunk the myth of the techno-savvy child, which only obscures the need for increasing the digital skills of children, while also documenting with solid evidence the need for increasing a participatory, child-inclusive approach to children’s safety online (only 36% of children said it is “very true” that they know more about the internet than their parents).

In addition to this, the child as perpetrator of problematic, violent, even premeditated acts, as disconcerting as the idea might be, highlights important implications: the corrosion of a discourse of innocence on one hand, and a break with the unified conception of “the child” and “childhood”, on the other.

A revision of the adequacy of protectionist views (of children as victims) versus the view that stresses the participation of children (children as competent agents) must be undertaken with specific online risks in mind. The following section reviews relevant EU internet safety policy pronouncements taking this distinction into account.

**Early Policy Discourses, 1996-1998**

The period between 1996-1998 marks the beginning of an explicitly protectionist approach in policy related to children’s use of the internet. The European Commission passed the first legal acts that made direct reference to the risks

The Communication on “Illegal and Harmful Content on the Internet” offered a general approach that distinguished between “illegal content” versus “harmful content”, indicating parents as the “locus” of control in regulating children’s internet access. Thus, the parents were defined as being responsible for preventing children’s exposure to and consumption of “harmful content” on the internet. The Green Paper presented in detail the mechanisms for the protection of minors at three levels: the level of information providers, access providers and the user. Apart from its identification of users, parents were considered solely responsible for limiting and preventing access of their children to harmful content (the case of “restrictions on computer use” and “memory storage of navigation on the networks”) (p. 20) – or more precisely, what the “Green paper” referred to as “parental control”. Finally, the paper indicated the need for a campaign of awareness-raising and education related to the protection of minors and stated that the “targets” of such action would be both parents and their children. As in the case of the Communication, in the “Green Paper” only parents were credited with the means for preventing the access to and the use of harmful content of the Internet.

The exclusive emphasis placed on “parental control” of children’s access to internet content is to be found in other internal documents of the European Commission in this period. Despite the “fixation” on the general theme of “parental control” (that is, on considering children only as “innocent agents”), it is worth noting that policy documents briefly mentioned, for the first time, children’s responsibility in using the internet when it made the recommendation to Member States to promote “measures that enable minors to make responsible use of new audiovisual and information services”.

A further “Action Plan” released in 1997 was based on the conceptual distinction between two types of internet content (e.g. “illegal” and “harmful”) and contained action lines on creating a safe environment on the Internet. In the second chapter (“The political consensus for action”), the plan repeated the understanding of children “as innocent victims” by granting the responsibility of dealing with harmful content to parents, without mentioning children as possible partners in these joint actions.

The “Council Recommendation 98/560/EC on the development of the competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity” represents a turning-point in the understanding of children in relation to illegal and harmful content. The Recommendation is the first European document that promotes a more balanced
accent on two types of “responsibility” in dealing with illegal and harmful internet content: responsibility of the parents and (a new one) that of the children (“minors”). The hierarchical view of the parent’s role (previously stated only as “control” from above that had to be exercised on the “helpless” child) was replaced in the Recommendation’s text by a more horizontal understanding of the relation between parents and their children.

Policy Development, 1999-2004/5

The implementation of the “Safer Internet Action Plan” (1999-2003) marked the first active intervention in the field of child protection against illegal and harmful content on the Internet. Debate at European Parliament level had identified areas for concrete measures related to the internet where Community resources should be focused and “defined four specific objectives: the creation of a safer environment (through a network of hotlines and the adoption of codes of conduct), the development of a filtering and rating system, the encouragement of awareness-raising actions, and other supporting action” (Casarosa 2010: 4-5). The distinction between two types of “bad” content on the internet (e.g. harmful and illegal) was maintained, as was the distinction between children’s access to and use of the internet content, on the one hand, and, on the other, the necessity of “protective” measures (by parents, educators and social workers) aimed at controlling minors’ access to inappropriate online content. Thus, the perspective on children-parents/teachers’ relation remained a “protective” one, the locus of control for internet access having been entrusted to adults who were considered as the only ones able to “decide” on the type of content to which the children would have access. While only parents and teachers were considered able “to decide” about internet content (and, as such, were in a superior position to children), the third paragraph (Article 2, p. 1 33/3) places children and parents/teachers on the same level by making reference to “raising the awareness” related to internet risks, and considering children as “users of the internet industry’s services”.

Internet Safety Policy, 2005-2008

In 2005, the European Commission proposed and adopted a new mandate for an extended Safer Internet Action Plan (2005-2008) (Decision No 854/2005/EC). The decision marked a new step forward, replacing the “paternalist” (“protective”) view of children and their relation with (illegal and harmful) internet content with a more “proactive” one, based on children’s awareness, first of all, and the recognition of their capacity to act in a responsible manner in re-
lation to internet content. The starting point of the decision was, once again, the existence of illegal and harmful internet content and, for the first time, the concrete measures for promoting safer internet use were addressed not only to adults but, equally, to children. Thus, in article (7) of the decision’s “Preamble” (p. L 149/2), it was stated that the target groups for the practical measures still needed in this domain were “parents and children” – an equality of status never met before within the European Commission’s proposals. The general view of children in the document’s text was a changed one. With Article 1, the decision went a step further from the “protective” view and stated that the main objective the new programme had to address was: “the issue [of] safer use of the Internet and new online technologies, particularly [for the] children.”

Other Recommendations (“Council Recommendation 98/560/EC on the development of the competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity” and “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”) adopted in 2006 by the European Parliament and the Council of Europe stated the centrality of protection of minors and (this time) explicitly introduced children as among the beneficiaries of the Safer Internet Programme’s action lines. The emphasis placed on the aim of teaching children how to “effectively use” the internet marked a progression from previous positions. It was the first time a document of the European Union referred to children’s relation to internet content from a “utilitarian” (“pragmatic”) point of view, by granting them the ability to do things in an “effective” way – that is, children’s actions could have clear, observable and measurable effects as is the case with activities carried by adults (parents, teachers or other persons). In the same vein as previous European Commission policy since 1996, the Recommendation granted responsibility of reporting and assessing the illegality or harmful character of internet content for adults (parents, teachers and trainers).

The Recommendation maintained, as such, the earlier distinction between children and adults in the decision establishing the multiannual Safer Internet Programme (OJ L 149, 11.6.2005): only parents, teachers and other adults could “responsibly” assess the (“good” or “bad” – e.g. illegal and/or harmful) quality of internet content and they were entitled to do so for children’s benefit. A disjunction between “efficacy” and “responsibility” resulted: the most useful children’s actions related to internet content were not, per se, assessed as responsible – the result being a view (enclosed in the Recommendation) of children as active individuals but with a limited autonomy and ability to discern what is good or bad in the world around them.
The first objective explicitly related to children was that Member States had to promote actions “to enable minors to make responsible use of audiovisual and on-line information services” (p. L 378/74). It is true that in the case of this objective, adults (parents, teachers and trainers) were considered as the main target group of “awareness-rising”, but the introduction of the “responsibility in internet use” for children could be assessed as lessening the gap between adults and minors at least in the future. Second, the European Council’s document introduced, for the first time, a new relationship among different actors in the field: the direct link between the industry and children as beneficiaries of the industry’s products. This connection took the shape of recommendation that access filters to internet content should be implemented and developed by the industry by taking into account the needs of a new type of user: the child.

Similarly, we tried to assess this tendency in offering a different view on children’s access and use of internet content on the basis of “intentions” enlisted by the European Commission in the recommendation’s text (p. L 378/75). Although the documents re-stated the maintenance of “parental control” in the field, of targeting awareness-rising actions towards parents and schools and of continuing the education of parents in the field of filter software efficacy, it also introduced a new dimension related to children: an internet domain specific to children that would respect their rights. In other words, under the condition of maintaining children’s right to “useful” acts but without granting them an equal degree of “responsibility” in internet-related behaviour, this intention could be judged as a step forward to a more “competent agent” view on children’s relations to internet content.

Internet Safety Policy, 2009-2011

Between 2006 and 2008, the European Commission (2006) made only one interim evaluation of the Safer Internet Plus programme (2005-2008) and a final evaluation of this programme in 2009 (European Commission 2009). The “Final evaluation” is important for our analysis because of the specific chapter on “Recommendations” made at the end of Safer Internet Plus programme implementation. It is true that the document did not have the legislative power of a European Commission “Decision” or “Recommendation” but a step further toward a more “active” view on children’s relation with the internet content is evident. Two key elements were important in this respect. We refer here, in the first case, to the introduction of children’s right to take an active part in the process of discussing issues of safer internet – recommendation (1) (p. 2 and p. 55). And, secondly, we noticed that in the text of the Recommendation (8) (p. 3 and p. 56) a new perspective on childhood was introduced: the child who had displayed criminal online behaviour.
At the end of the Safer Internet Plus programme, in 2009, the Council of Ministers adopted the new Safer Internet Programme proposed by the European Commission for the period 2009-2013. As in the case of previous European Safer Internet Plans, the starting point of the 2008 European Commission’s position was, once again, the existence of illegal and harmful internet content and the need of a safer internet for children. As expected, the documents made references to the previous documents of the Safer Internet Plans and, at the same time, contained some new elements that represented an advancement toward a more “active” view of children’s relationship with internet content. The need for “positive [internet] content for children” was introduced for the first time in a European document. In addition, if in the “Recommendation 2006/952/EC”, children were (a priori) entrusted with the ability to act “effectively” in relation to the internet, in the 2008 Decision their internet-related actions had to be, at the same time, “effective” and “safe”. By reaffirming the “utilitarian” approach to children, the document seemed to add a new quality: the child had the ability to discern between “safe” and “unsafe” content and, from here, it would be supposed that he or she could act in a safe (not only effective) manner, just like adults (parents, teachers, carers and educators). As such, it was not surprising that in the whole decision’s text (not only in its “Preamble”) the missing key element was “parental control”. This omission could be considered as essential for its new perspective on children and parents’ relations to internet content and was made clear in Article (1) (“Objective of the programme” – p. L 348/120) when the first definition of “child” was offered in the entire history of the regulations devoted to children’s safety on the internet (1996-2009):

[3. For the purpose of this Decision] ‘children’ means persons under 18 years of age, unless the relevant national law confers on them, under certain conditions, full legal capacity under that age (p. L 348/120) (bringing this into line with UNCRC).

In sum, the decision’s corpus (text) represented a real break with the old view of “children” as helpless individuals, placed under the parents’ control, unable to access and to use the internet in an independent way. As odd as it may seem, until 2008 no definition of the main term of any regulation referring to children and internet safety, that is, the “child” was given. Only from 2008 was it clear that “child” referred to individuals who were in parents’ or carer’s economic and social charge. At the same time, due both to the weakening of parental control – “control” in this case being understood as a “filter” between the children’s action and the internet’s world – and addition of “safety” as a desired trait of children’s acts (that was assessed since 2006 as “effective”), it became possible for further regulation to ascribe autonomous legal status to the individual labelled as “child” in relation to internet use.
The decision’s break with the “protective” view of the child was clear in the “Annex” corpus where future “Action lines” of the Safer Internet Programme were presented. The newly-introduced “equality” of status among children, parents, teachers, educators was made clear from the beginning, all the above-mentioned categories being treated as future targets of educational activities related to fighting against illegal and harmful internet content. Moreover, compared to previous European programmes from 1999 and 2005, the main objective of the 2008 programme was a “child-centric” one: “to promote safer use of online technologies, especially by children” — the fact that the reference to adults was an implicit one placed parents, teachers or educators in a secondary role. Children were explicitly mentioned as the target for concrete measures, were described as individuals able to act (at least in the future) in a responsible way in relation to internet content and were linked to industry through the idea of a “positive [internet] content for children”.

To the above-mentioned traits ascribed to the child (ability to act responsibly and safely), the actions incorporated in this approach added a new one: children’s active involvement in solving the issues of safer internet content, their capacity to define the world outside them in a way that is worth consideration by “others” (e.g. adults).

With “Decision No. No 1351/2008/EC” and the new Safer Internet Programme (2009-2013), the break with the old “protective” view on children was complete. Together with the Final evaluation of the implementation of the Safer Internet Plus programme (2009), the European Commission Decision from 2009 draws a different image of the child: being defined as a “legal subject” and belonging to a clear age-group (individuals under 18 years old), he or she is no longer under total “parental control” (although it remained in parents’ or carer’s economic and social charge). The child is an individual that could act in a “effective” and “safe” way with regard to the internet and who had his or her own view of various issues related to online content (and, implicitly, safety). He is no longer only a “victim” of others (e.g. adults) but, equally, could be an “aggressor”. In other words, the child not only instrumentally uses the internet but (can) become co-author of “good” or “bad” internet content.

‘Promoting Participation’:
EU Kids Online Policy Recommendations

Arising from its survey of children’s use of the internet across Europe, one of the key policy recommendations advanced by EU Kids Online was the raising of awareness among parents about internet safety matters given the wide gaps in knowledge found about risks children face online (O’Neill and McLaughlin 2010: 3). Despite (initial) EU policy efforts which stressed the importance of
“parental control” over a more child-inclusive, participatory approach, a lot of European parents, it would appear, still remain in the dark when it comes to protecting their children online. In addition, parents’ prioritizing of schools, traditional media and family/friends over the use of online sources of information regarding online safety, coupled with the low usage of internet safety tools, implies also that many parents are ill-equipped to assume the role of online safety watchdog so optimistically assigned to them by initial EU policy. Instead, findings show a majority of parents still in need of awareness and digital literacy to enable them to assess and deal with the online challenges faced by their children.

Debates on the role of parental authority have led scholars to question whether such control is beneficial or detrimental to children (Grolnick 2003: x-xi), with the latter perspective gaining increasing support in light of recent approaches to children’s agency. Advances in socialization theory have moved the discussion from a unidirectional perspective to a bidirectional one, building on transactional models of relationships where the agency of the child is recognized (Kuczynski 2003). From a theoretical point of view, this is an approach strongly endorsed by the framework of EU Kids Online. While restrictive parental mediation of children’s internet use leads to fewer risks, it is also a type of mediation that limits internet use in general, thus depriving children of many online benefits, such as learning, participation, communication and opportunities for fun (Duraeger and Livingstone 2012).

Another key recommendation was the need to focus online safety efforts on young children, since they are the ones that are most likely to experience harm as a result of online risk investigated in the project, such as exposure to sexually explicit materials (Livingstone and Görzig 2011) or going to offline meetings with people first met online (Hasebrink, Görzig, Haddon, Kalmus and Livingstone 2011). The decreasing age for going online for European children, (average age of 9 years according to EU Kids Online), coupled with the high frequency of use (93% going online at least weekly) are more reasons for targeting younger children.

Children's digital citizenship was another topic addressed in policy recommendations made by EU Kids Online (O’Neill and McLaughlin 2010: 4-5). More privatised and independent use, away from adult supervision, calls for better self-protection and responsible internet use by children. The agency perspective, which views children as competent, participatory actors in the digital landscape, needs to be moderated by the need to ensure children have the ability and the skills (both informational and safety skills) to protect themselves online. The myth that all children are techno-savvy only obscures the need for enhancing their digital skills. The perception that children know more about the internet than their parents has, according to EU Kids Online, been exaggerated: only 36% of 9-16-year olds said it was ‘very true’ that they know more about the
internet than their parents; two in three of the younger children (aged 9-10 years) said ‘it’s not true’ (Livingstone, Haddon, Görzig and Ólafsson 2011a).

The myth that all children are in constant need of adult protection is similarly debunked by EU Kids Online findings and cannot account for situations where the child is also a perpetrator of malicious or even criminal acts, online or offline. Findings show that most of those who bully – online or offline (60%) – have themselves been bullied by others, and 40% of those who bully online have themselves been bullied online. Psychological vulnerability was evidenced in the case of both those who bully and who are bullied online, indicating a cycle of behaviour that damages both victim and perpetrator (Livingstone, Haddon, Görzig and Ólafsson 2011a). Again, stronger participatory policy measures targeted at the most vulnerable (online and offline) that emphasise the child’s responsible, sensitive and ethical behaviour towards others online, are urgent.

The highest danger perpetuated by a protective-restrictive approach is the illusion of its own efficacy. For example, in a protective-restrictive framework, age restrictions related to setting up a profile on a social networking site should be sufficient to keep children away from services not designed for their age group. In reality, however: 38% of European children 9-12 year olds declare having an SNS profile (Hasebrink, et al. 2011). Similarly, 46% of American 12-year-olds report having a SNS profile (Lenhart, et al. 2010). Since many “underage” users register with a false age, half the time with the knowledge and sometimes with the help of their parents (boyd, Hargittai, Schultz and Palfrey 2011), it is clear that a (predominantly) restrictive framework on its own is not enough and needs to be balanced by a more honest, inclusive and realistic approach that acknowledges the child’s own needs and preferences, even if they differ from policy-approved ones. Parents, it would appear, are willing to help their children violate the age-restrictive measures if they see it as enhancing their children’s educational objectives, as enabling family communication, or as fostering their children’s social interactions (boyd, et al. 2011).

Needless to say under the circumstances, turning a blind eye and failing to take into consideration the children’s agency (which in this case manifests itself in the form of circumventing age-restrictive measures on SNSs and adult authority in general) will only result in unintended consequences and younger children taking more risks online.

Due to the different levels of inter-generational digital divide (the difference between parents’ and children’s digital competencies) experienced in countries across Europe, policy initiatives that promote digital literacy should be targeted particularly at Eastern European countries, where parents’ skills lag massively behind those of their ‘digital native’ children. Also, previous research has shown that parents in European countries with collectivistic values impose restrictions on time spent online more often than parents in countries with individualistic values (Kirwil 2009).
It is especially in countries such as Romania, Bulgaria, Poland, Lithuania and Turkey, where the practical failings of protective-prohibitive policy discourse are most exposed: ill-equipped and unaware parents rely heavily on restrictive mediating strategies (Kalmus and Roosalu 2010) that might be either circumvented by their more techno-savvy children or hinder children’s taking up of online opportunities (Kirwil, Garmendia, Garitaonandia and Martinez Fernandez 2009). Although restrictive mediation reduces harm (Hasebrink, et al. 2011: 13), it also reduces general use and opportunities. Moreover, children who undertake fewer activities online are likely to experience more harm (in the case of exposure to sexual images and sexual messages), as reported in Hasebrink, et al. (2011: 54).

However, in the same countries, children themselves, especially younger ones, report low levels of digital skills, a fact that indicates the need for prioritizing digital literacy and online safety in national educational curricula. Also, parental education has been linked to higher skills and online activities among children (Hasebrink, et al. 2011: 13), which in turn, have been connected to higher resilience and more effective coping strategies. As a consequence, increasing e-literacy and digital education of parents would appear to be an effective course for policy action.

One can envisage that children are unlikely to seek support or talk to restrictive, ‘closed-minded’ and digital illiterate adults. Parents are often a second choice when it comes to children sharing an unpleasant online experience and sometimes no choice at all (O’Neill and McLaughlin 2010: 23). However, children do welcome parental guidance and mediation, but one can assume that they are more likely to seek it if they deem it reliable. Situations in which parents are not the primary choice for guidance and safety advice suggest a communication/trust gap that hinders a positive parenting role in increasing online safety. The situation calls for a blending of protective and empowering measures, whereby parents need to be empowered to be able to protect and children need to be empowered in order to protect themselves.

However, findings from EU Kids Online also support the major role of peers as an important locus of support, whatever the type of risk. In addition, peer mediation is strongly related to children taking up more opportunities online, better digital skills, as well as more online activities (Hasebrink, et al. 2011: 60, 65). Peer mediation is, therefore, one of the major online safety resources still untapped by policy measures.

Conclusions

Evidence gathered by EU Kids Online confirms that support and enablement, rather than control and restriction should be the emphasis of policy measures in internet safety. Relying solely (or mostly) on restrictive measures and ‘pa-
rental control’ is the equivalent of banning cycling as a means of preventing accidents (Livingstone, _et al._ 2011b: 12). Similar to the normative distinction between what constitutes “good” and “bad” activities online, the distinction between risk and harm should be a sensitive one that incorporates the view of children’s agency and their different levels of development. Rather than treating children as a monolithic bloc, protective policy measures should be directed at the most vulnerable and youngest children, without undermining their participation rights and access to online opportunities.

For purposes of comparison, the model of Four Constraints – architecture, law, market and social norms – advanced by Lawrence Lessig (2004) to explain the regulation of cyberspace might also be useful in reshaping the tension between protective and enabling approaches to internet safety. The constant changing nature of the architecture (of the digital landscape), coupled with lower costs of entry and access to digital content (market) has marked the beginning of unprecedented exposure of children to various types of online content and contact, some of which are risky or harmful. Social responses (e.g. protective, restrictive, the ‘social norms’) and the law (policy measures) have coupled to ensure that protection has tended to dominate, sometimes at the expense of a more participatory, child-inclusive approach. However, policy measures and social norms can no longer afford to ignore children while claiming to protect them. A fifth dimension, that of children’s participation rights needs to be added to the picture.

As a key recommendation of the EU Kids Online project, the emphasis on empowerment rather than restriction and the encouragement of young people’s self-protective, responsible, self-governing behaviour (O’Neill, Livingstone and McLaughlin 2011) are the appropriate steps to ensure children’s participation rights in the digital landscape. Denying children the opportunity to take responsibility for their actions online will only delay them their ability to do so, and thereby perpetuate the cycle of victimization-protection-restriction.

Notes

2. The articles of the “Convention on the Rights of the Child” refers at the children’s right to life (article 6); the children’s right to participate in all matters affecting them, and those views should be given due weight “in accordance with the age and maturity of the child” (article

Acknowledgements

This chapter draws on the work of the EU Kids Online network funded by the EC Safer Internet plus Programme (project code SIP-KEP-321803) and was supported by the VITOVIN project (CZ.1.07/2.3.00/20.0184), which is co-financed by the European Social Fund and the state budget of Czech Republic.
12); children’s right to get and to share information (article 13); the children’s right to privacy (article 16) and the children’s right to reliable information from the mass media (article 17) (“Convention on the Rights of the Child”, available at: http://www2.ohchr.org/english/law/crc.htm, accessed on the 10th of March 2012).


8. The paragraph referred to is: “In response to public demand, a number of technologies have been developed over the past two years to enable parents to control Internet content coming into their homes. Contrasting with “upstream censorship” by official agencies (preventing illegal content from being published at all), filtering provides for “downstream control” by parents (preventing harmful content from reaching minors). The filtering model – which stresses the parental responsibility rather than government intervention – is strongly advocated by the industry and the civil liberties group as the most effective way of solving the specific challenges of the Internet and of taking into account the differences in standards of taste and decency between countries, communities and families”.

9. The paragraph is: “Parents and children must learn to use the new communication tools. They need to be warned of the new risks involved and also of the protection facilities available. Information, awareness-raising and education are the keys to effective protection of minors and to establishing the climate of confidence on which the development of the new services depends.” (p. 20).


13. The paragraph is: “[The Council of the European Union recommends to the Member States to] promote, in close cooperation with the parties concerned, measures to enable minors to make responsible use of new audiovisual and information services, notably by improving the level of awareness among parents of the potential of the new services and of the means whereby they may be made safe for minors; facilitate identification of, and access to, quality content and services for minors, including through the provision of means of access in educational establishments and public places”. (see the document at: http://ec.europa.eu/avpolicy/docs/reg/minors/comlv-en.htm#%284%29)
15. The paragraph is: “In tackling harmful content, the priority actions should be enabling users to deal with harmful content through the development of technological solutions (filtering and content rating systems), to increase parental awareness, and to developing self-regulation which can provide an adequate framework, in particular for the protection of minors”. (p. 3)
17. The Article is: “[The European Commission] Hereby recommends that the Member States foster a climate of confidence which will promote the development of the audiovisual and information services industry by: […] (4) promoting, in order to encourage the take-up of technological developments and in addition to and consistent with existing legal and other measures regarding broadcasting services, and in close cooperation with the parties concerned: action to enable minors to make responsible use of on-line audiovisual and information services, notably by improving the level of awareness among parents, educators and teachers of the potential of the new services and of the means whereby they may be made safe for minors; action to facilitate, where appropriate and necessary, identification of, and access to, quality content and services for minors, including through the provision of means of access in educational establishments and public places.”
20. The paragraph referred to is: “In order to attain the objective referred to in Article 2, the following actions supporting and promoting measures to be taken in the Member States shall be undertaken under the guidance of the Commission, in accordance with the action lines set out in Annex I and the means for implementing the action plan set out in Annex III: […] encouraging industry to provide filtering tools and rating systems, which allow parents or teachers to select content appropriate for children in their care while allowing adults to decide what legal content they wish to access, and which take account of linguistic and cultural diversity”. (p. I 33/2)
21. The paragraph referred to is: “In order to attain the objective referred to in Article 2, the following actions supporting and promoting measures to be taken in the Member States shall be undertaken under the guidance of the Commission, in accordance with the action lines set out in Annex I and the means for implementing the action plan set out in Annex III: […] increasing awareness of services provided by industry among users, in particular parents, teachers and children, so that they can better understand and take advantage of the opportunities of the Internet”. (p. I 33/2) Meanwhile, when actions regarding the increase in “awareness” were presented in detail (Action line 3, “Encouraging awareness actions”), children were maintained in a subordinated and helpless position.
22. The article referred at is: “Practical measures are still needed to encourage reporting of illegal content to those in a position to deal with it, to encourage assessment of the performance of filter technologies and the benchmarking of those technologies, to spread best practice for codes of conduct embodying generally agreed canons of behaviour, and to inform and educate parents and children on the best way to benefit from the potential of new online technologies in a safe way” (p. I 149/2).
23. See for example European Decision No 276/1999, “Action line 3” (p. I 33/8), which had stated as “target-groups” for the “Safer Internet Plan” “parents and teachers” (e.g. the “aware-
ness actions” had been addressed to them in the first European Union plan for promoting safer internet).

24. The article referred to is: “1. This Decision establishes a Community programme for the period 2005 to 2008 to promote safer use of the Internet and new online technologies, particularly for children, and to fight against illegal content and content unwanted by the end-user.” (p. L149/2). One could notice, as such, the absence of parents and teachers in relation to the main objective of the European Commission’s program from the beginning and the (almost) unique stress put on children’s safety in using the internet.

25. The Article referred at is: “(11) The changing media landscape, resulting from new technologies and media innovation, makes it necessary to teach children, and also parents, teachers and trainers to use audiovisual and on-line information services effectively.” (p. L 378/73)


27. The Article referred to is: “(14) The Commission encourages cooperation and the sharing of experience and best practices between existing self-and co-regulatory bodies, which deal with the rating or classification of audiovisual content, regardless of the means by which it is delivered, with a view to enabling all users, but especially parents, teachers and trainers, to report illegal content and assess the content of audiovisual and on-line information services, as well as any legal content which could harm the physical, mental or moral development of minors.” (p. L 378/73)

28. One can notice that the old “protectionist” (“parent-centred”) view (preeminence in the European Commission’s legal acts until now) was abandoned but it was not replaced with “total competent agent” perspective. In the case of this document this complete replacement of view on children in relation to internet content was not possible at that moment and, from here, it was postponed after the fulfilment of some general objective directly related to rising children’s responsibility in using the internet.

29. The Article referred to is: “Hereby recommend that: I. The Member States, in the interests of promoting the development of the audiovisual and on-line information services industry, take the necessary measures to ensure the protection of minors and human dignity in all audiovisual and on-line information services by: […] 2. promoting, in order to encourage the take-up of technological developments, in addition to and consistently with existing legal and other measures regarding broadcasting services, and in close cooperation with the parties concerned: (a) action to enable minors to make responsible use of audiovisual and on-line information services, notably by improving the level of awareness among parents, teachers and trainers of the potential of the new services and of the means whereby they may be made safe for minors, in particular through media literacy or media education programmes and, for instance, by continuous training within school education.” (p. L 378/74)

30. The Article referred at is: “Hereby recommend that: II. The audiovisual and on-line information services industry and other parties concerned: 1. develop positive measures for the benefit of minors, including initiatives to facilitate their wider access to audiovisual and on-line information services, while avoiding potentially harmful content, for instance by means of filtering systems.” (p. L 378/75).
31. The Article referred to is: “Take note that the Commission: 1. Intends to promote, in connection with the 2005-2008 multiannual Community programme on promoting safer use of the Internet and new on-line technologies, information actions aimed at citizens Europe-wide using all communications media, to inform the public about the benefits and possible risks of the Internet, how to use it responsibly and safely, how to make complaints and how to activate parental control. Specific campaigns could be aimed at target groups such as schools, parents’ associations and users.” (p. L 378/75)

32. The Article referred to is: “Take note that the Commission: 2. intends to explore the possibility of introducing a European freephone number or of extending an existing service to assist Internet users by directing them to available complaint mechanisms and information resources and providing information for parents about the effectiveness of filtering software.” (p. L 378/75)

33. The Article referred to is: “Take note that the Commission: 3. intends to explore the possibility of supporting the establishment of a generic second level domain name reserved for monitored sites committed to respecting minors and their rights, such as .KID.eu.” (p. L 378/75)

34. The Recommendation referred to is: “1. The rights and privacy of children, young people and other legitimate Internet users should be protected and promoted within all activities of the Programme. The involvement of young people themselves in discussion, design and delivery of solutions could be further intensified.” (p. 2 and p. 55)

35. The Recommendation referred to is: “8. Further knowledge enhancement activity could be conducted in two key areas: problematic, risky and criminal online behaviours on the part of children and young people themselves; the underlying reasons for the trends identified by INHOPE in respect of illegal content.” (p.3 and p. 56)


38. The Article referred at is: “(10) The programme should further support measures to encourage positive content for children.” (p. L 348/119)


40. The Article referred at is: “(11) The changing media landscape, resulting from new technologies and media innovation, makes it necessary to teach children, as well as parents, carers, teachers and educators, to use on-line information services safely and effectively.” (p. L 348/119)

41. The Paragraph referred at is: “The objective of the Programme is to promote safer use of the Internet and other communication technologies (‘online technologies’), to educate users, particularly children, parents, carers, teachers and educators in this regard and to fight against illegal content and harmful conduct online. (p. L 348/120)

42. The Paragraph referred to is: “The Programme has the overall aim to promote safer use of online technologies, especially by children, promote the development of a safe online environment, reduce the amount of illegal content disseminated online, tackle potentially harmful conduct online (including the psychological manipulation of children with a view to sexual abuse and ‘grooming’, which is the process by which an adult befriends a child with the intention of committing sexual abuse, electronic harassment and electronic files showing physical and/or psychological aggression) and ensure public awareness of online risks and precautions, as well as to develop pedagogical tools on the basis of sound practices.” (p. L 348/122)

43. See in this respect the document’s “Preamble” (p. L 348/119) where this concept was introduced for the first time in a European document.
44. The Article referred to is: “The activities will aim to bring together stakeholders so as to promote a safer online environment and protect children from harmful content. The main planned actions are: [...] 4. Stimulating the involvement of children in creating a safer online environment. [...] Actions will aim to involve children, ensuring equal participation of girls and boys, with the aim of better understanding their views and experiences concerning the use of online technologies and, with the support of specialists, of promoting a safer online environment for children.” (p. L 348/124)

45. ‘Bookmarking a webpage’ is an example of information-related digital competence, while ‘blocking someone you don’t want to hear from’ is a safety skill, distinction operated also by Hasebrink et al. (2011).

References


Part III
Policy Paradoxes
Chapter 13

Risk versus Harm

Children’s Coping Profiles

Leen d’Haenens & Liza Tsaliki

Recent developments in the media have reinforced changes taking place in childhood with the effect of blurring the boundaries between children and adults: new media technologies allow children access to material previously restricted to adults, as they make what Neil Postman calls ‘adult secrets’ available to children to a greater extent than broadcast television ever did (Buckingham 2000: 99). Children are targeted as autonomous consumers with disposable income; they can communicate more easily with each other (and with adults) without having to identify themselves as children; even in the material produced exclusively for them, they become acquainted with aspects of life that were previously considered unsuitable for children. As their technological aptitude increases, children no longer need to watch or read what their parents choose – instead, they have developed particular cultural competencies (‘media literacies’) that are exclusive to them. As a result, they may share a global media culture with other children and increasingly less with their parents. New media also make it possible for children ‘readers’ to write their own texts and rewrite existing ones. Constraints of geography as well as social hierarchies no longer apply as the new media are open to all children (who can afford them). The boundaries between children themselves are being reconfigured as older children can no longer be ‘protected’ from experiences seen to be morally damaging or developmentally unsuitable, while younger ones increasingly take part in worlds that are inaccessible to their parents (Buckingham 2000).

These new technologies have, without a doubt, brought hitherto inaccessible means of cultural expression and communication within children’s reach, and in this context, they have contributed to the ongoing social construction of the ‘child at risk’, whether that may be the result of sensationalist press stories or academic research. This notion of the ‘child at risk’, is a sentimental construction of children as innocent and vulnerable, and thus in need of adult protection; opposite it stands yet another sentimental construction of childhood, one that sees children as ‘media-wise’ and active bearers of a natural wisdom that
guides them in their relationship with new media and technologies. However, both of these conceptions, the vulnerable child and the media-wise one, derive from essentialist constructions of childhood and of the new media, and treat the child as an isolated individual consciousness instead of providing a social understanding of the relationship between children and the media. Buckingham (2004) is careful to stress the fatalism and polarization between the two positions through which we make sense of children’s relationships with the media (old and new) – if one is false, then the other one is, by default, true.

The implication, however, is that reactions to the overdetermination of children by negative media effects run the risk of adopting an equally simplistic ‘child-centred’ approach, whereby the ‘media-savvy’, ‘active’ child becomes yet another stereotype to be endlessly celebrated (Buckingham 2000: 115). It can at least be said that such fascination with children’s active media use may make us overlook the fact that there are gaps in children’s knowledge that need to be addressed, and that children’s media literacy develops as they grow older on the basis of the critical perspectives that are available to them. In that respect, caution is needed so as not to romanticise the notion of the ‘media-wise’ child and turn the argument of children’s high levels of media literacy into a rhetorical platitude (Buckingham 2000: 116). In this light, we are also careful, in this chapter, not to reiterate the dichotomy between the ‘incompetent’ and the ‘competent’ child by either denigrating children and viewing them as incomplete adults or by attributing them an overwhelming degree of sophistication and autonomy. We argue, as others before us did (Buckingham 2000: 120), that we need to broaden our understanding of children’s relationships with the media by taking into account their social lives, as well as the broader material and symbolic conditions within which their media consumption takes place.

Yet, a debate concerning the exposure of young people to potentially ‘harmful’ or offensive media content continues, despite the fact that evidence of harm from media use is inconclusive. Far from being greeted as valuable educational tools, new media technologies have been treated with suspicion by many parents and educationalists. It has been argued that computers pose health hazards, create developmental problems, stunt the imagination, isolate children from the adult world (Alliance for Childhood 2000, cited in Livingstone 2003: 154), and provide a haven for pornography and paedophiles. Evidence from the EU Kids Online project (Haddon and Stald 2009) suggests that press coverage detracts attention from the potential benefits of the internet to focus public attention disproportionately on the risks, thus promoting a notion of the internet as a scary and sinister place (Tsaliki 2011: 294). Things get more complex if we consider that the terms ‘harm’ and ‘offence’ are increasingly used in discussions of media and content regulation, gradually replacing ‘taste and decency’. According to the Oxford English Dictionary (2004), harm signifies ‘material damage, actual or potential ill effect’, whereas offence corresponds
to ‘an act or instance of offending; resentment or hurt, something that outrages
the moral or physical senses’. ‘Harm’ is generally perceived to be observable by
others, regardless of whether it is acknowledged by the individual concerned,
and thus to be reliably measurable. ‘Offence’, however, tends to be perceived
as something that is subjectively experienced and therefore difficult to measure

However, ‘the link between risks, incidents and actual harm is genuinely ten-
uous: not all risks taken result in worrying incidents, not all worrying incidents
result in actual or lasting harm’ (Livingstone 2003: 157). Many questions about
harm remain difficult to address because research offers evidence based on the
balance of probabilities rather than on irrefutable proof. Millwood-Hargrave
and Livingstone (2006) have called for multi-method, long-term, cross media
research on a diverse range of audience and user groups, arguing for the search
for simple and direct causal effects to be replaced by a risk-based approach
that takes into account a wide range of factors. Many of these are culturally
specific, for example, national traditions of content regulation, approaches to
parenting, and frames for judging content and offence. What is at stake, then,
is the likelihood of risk rather than of inevitable harm; in fact, current research
indicates that it is ‘vulnerable’ audiences that are more susceptible to being
negatively affected by various media (Tsaliki 2011: 295).

Who Adopts which Approach when Encountering what Risk? Children’s Coping Profiles in Relation to Online Risks
We look at the child as a self-mediator when exposed to online risks; the
mediating role of parents, peers and teachers will also briefly be taken into
account. Exposure to online risks, or online risky opportunities, as these have
been contextualized by the EU Kids Online project, (i.e. being bullied online,
seeing sexual images online, and receiving sexual messages online) may or
may not be harmful for those exposed. In fact, the majority of children, as has
been established by EU Kids Online research, will not necessarily experience
any negative effects. Exposure to online risks does not necessarily result in
harm as often most children respond in a positive (proactive) or neutral way
to these online experiences (Staksrud and Livingstone 2009). However, some
children prove to be more vulnerable than others after feeling bothered by
a potentially harmful situation online, as they experience more difficulties in
adopting an appropriate coping response (e.g., Vandoninck, d’Haenens and
Donoso 2010). Hence, a challenging question is to find out when risk of harm
turns into actual harm, and when it does not. In other words, what groups of
children are at risk of harm, and what children are just at risk? Keeping children
away from online risks is not a realistic strategy as this would mean they are
withheld from online opportunities to succeed as well. Hence, what implications should this have in terms of policy? Should policy be aimed at the many or at just the few? One of the main aims of the EU Kids Online research was to measure on a cross-national basis the incidence, distribution, severity and consequence of harm. This showed us that children’s personal characteristics have an impact on their perception of harm when exposed to online risks and the coping responses they choose to adopt.

This chapter will discuss the relative impact of socio-demographic (gender, age, SES), psychological factors (self-efficacy, sensation seeking and emotional problems) and children’s involvement in online activities on their self-mediated strategies as ways of coping with online risks and risky opportunities. Coping responses are inevitably linked to the child’s experience of adversity (Did you feel bothered?) and perception of harm. The latter is measured in terms of severity (How upset were you?) and duration (For how long did this feeling persist?).

Research on coping has yielded several ways of classifying types of coping strategies, for instance, between ‘system-based’ and ‘user-based’ approaches (that is, between technical solutions and parental guidance), or ‘restrictive mediation’ and ‘instructive mediation’ (that is, between rule-making and active efforts to interpret media content for children) (for an overview, see Kirwil et al. 2009). On the basis of these distinctions, various typologies of parental mediation of children’s internet use have been proposed. Lwin et al. (2008) identify four parental strategies: restrictive, promotive (only instructive mediation), selective (both restrictive and instructive), and laissez faire (no mediation). Livingstone and Helsper (2008) argued for four factors of parental mediation: an active ‘co-use’ and three types of ‘restrictive mediation’ (use of technical filtering/monitoring tools, rule-making and monitoring of visited websites and e-mails).

Kirwil et al. (2009) have identified individual-level differences depending on the child’s gender and age, and between parents based on their gender, education and internet use. In fact, they have shown that the more parents use the internet, the more they practice social mediation and apply restrictions (with the exception of parents who use the internet daily). Having said that, several researchers agree that in addition to individual-level variation in parental strategies, systematic cross-national differences exist (see Kalmus, et al. 2009, Kirwil 2009; Kirwil, et al. 2009; Livingstone and Haddon 2009; Lobe, et al. 2009). Following the socialization approach which situates parental practices in relation to socialization cultures, Kirwil et al. (2009) have interpreted cross-cultural similarities and differences in parental mediation by taking into account countries’ orientation in terms of individualistic and collectivistic values, something congruent with a long tradition of research on techniques and practices of child-rearing guided by parental values and attitudes, which, in turn, are influenced by broader cultural ideologies. They suggest, in broad terms, that parents from individualistically-oriented child-rearing cultures (e.g.,
RISK VERSUS HARM

historically Protestant Nordic Europe) engage more in all types of mediation, while parents from cultures with a collectivistic orientation (e.g., Portugal and post-communist Europe, excluding Slovenia) either do not use any mediation or favour restrictive rules or technical solutions. Kalmus and Roosalu (2011) also take up the socialization approach to parental mediation but assume, however, that the factors behind cross-national differences in parental strategies are multilateral. They argue that besides individualistic and collectivistic values, other cultural factors need to be taken into account; they also include the level of internet use among EU parents as it is a necessary precondition for applying technical restrictions. More importantly, they enhance our understanding of cross-national differences in parental mediation by taking into account institutional arrangements, such as gender embedded – or reflected – in welfare state typologies. The authors assume that the extent to which parents mediate their children’s internet use is influenced, among other factors, by the distribution of child-rearing tasks between the private and the public sphere as well by predominant gender role models in a given country (Kalmus and Roosalu 2011).

Notwithstanding the variety of mediation typologies, a one-size-fits-all coping approach, fit for all online risks, does not emerge from our data, as will be shown below. Specific risks ask for a specific response, so it seems, depending on both socio-demographic and socio-psychological characteristics of the child. Here, we distinguish between three types of coping approaches young people may use in order to protect themselves from unwelcome content or contact. Both the communicative and proactive approaches are problem-focused and can be labelled as ‘active’ coping strategies. Fatalistic strategies, such as hoping the problem disappears and stop using the computer, are considered to be passive strategies.

Communicative Approach

The most frequently adopted response among children when facing online risks is the communicative approach, seeking social support and talking with someone. For all online risks, children prefer talking to their peers (63-68%) or parents (48-54%). A minority talk to their siblings (14-18%), and only a few children turn to other persons such as teachers (4-10%) or professional childcare workers (2-4%) for advice on online risks. Overall, talking is the most favoured coping strategy. About half of the children will talk to somebody when confronted with upsetting sexual images. Six in ten will do this when receiving unwelcome sexual messages, and an overwhelming 77% report talking to somebody when a victim of online bullying. Girls, young people who are not into sensation seeking, and those children feeling upset for longer and more intensely, tend to look for solace in reaching out to significant others to talk
to (mainly their parents or peers). Younger children will be more likely to talk when they encounter upsetting *sexual images* or *sexual messages*. Remarkably, children with rather less digital skills are more likely to talk when they have fallen victim to *online bullying*.

Strikingly, children with emotional problems or low self-efficacy are not more likely to talk about their negative experiences compared to children without psychological issues. Individual psychological traits such as emotional well-being and self-efficacy are related to children's offline coping capacities. Children not feeling troubled and believing in their own self-efficacy, display more resilience when confronted with a stressful or disturbing situation. Besides personal characteristics, family and external support factors have an impact on resilience building in the face of stress and risk (Smith and Carlson 1997). Recent research on online coping strategies suggests that psychological factors related to offline resilience also come to play an important role in the display of resilience and coping behaviour when exposed to online risks and experiencing subsequent harm (Vandoninck, d’Haenens and Donoso 2010).

**Proactive Approach**

Second, children may also choose to engage in proactive strategies. These can be general, by having the intention of ‘trying to fix the problem’, or internet-specific, by ‘deleting unwelcome messages’ and ‘blocking the person who sent the messages’. Such an internet-specific proactive approach requires minimal digital skills, and may either result from a higher level of coping (i.e. relying on a broader range of capacities to fix the problem), or a higher level of feeling bothered or emotionally disturbed (i.e. possibly feeling more sensitive or less indifferent towards an upsetting experience).

Children respond most proactively when they are a victim of *online bullying*, with 36% trying to fix the problem. As to sexual messages (27%) and sexual images (22%) the tendency to fix the problem is less prominent. In general, children who are self-efficient and (fairly to very) upset are also more likely to adopt a proactive attitude. When confronted with online sexual risks, more digitally competent children also more often take up a proactive attitude. Internet-specific coping strategies (deleting unwelcome messages or blocking the sender) are practiced by about 40% of the children in case of a negative experience with sexual messages and online bullying. After feeling bothered by sexual images, only one in four young people delete the image or block the sender. Besides the clear impact of digital competences on the use of internet-specific coping strategies, no straightforward relationships emerge as to other personal characteristics.
Table 1. Variables Predicting a Communicative Approach based on All Children Who Have Been Bothered after Being Exposed to the Respective Online Risk in the Past 12 Months (%)

<table>
<thead>
<tr>
<th>Communicative approach</th>
<th>Sexual images (n=972)</th>
<th>Online bullying (n=1273)</th>
<th>Sexting (n=568)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boys</td>
<td>50(^a)</td>
<td>67(^c)</td>
<td>48(^c)</td>
</tr>
<tr>
<td>Girls</td>
<td>56</td>
<td>85</td>
<td>66</td>
</tr>
<tr>
<td>Age 9-10</td>
<td>61(^b)</td>
<td>78(^a)</td>
<td>NA</td>
</tr>
<tr>
<td>11-12</td>
<td>62</td>
<td>76</td>
<td>72(^c)</td>
</tr>
<tr>
<td>13-14</td>
<td>53</td>
<td>82</td>
<td>48</td>
</tr>
<tr>
<td>15-16</td>
<td>45</td>
<td>74</td>
<td>62</td>
</tr>
<tr>
<td>SES Low</td>
<td>60(^b)</td>
<td>74(^b)</td>
<td>61(^b)</td>
</tr>
<tr>
<td>Medium</td>
<td>46</td>
<td>82</td>
<td>52</td>
</tr>
<tr>
<td>High</td>
<td>57</td>
<td>73</td>
<td>70</td>
</tr>
<tr>
<td>SE Low</td>
<td>46</td>
<td>71</td>
<td>48</td>
</tr>
<tr>
<td>Medium</td>
<td>53</td>
<td>77</td>
<td>59</td>
</tr>
<tr>
<td>High</td>
<td>56</td>
<td>78</td>
<td>63</td>
</tr>
<tr>
<td>EP No</td>
<td>59</td>
<td>74</td>
<td>67</td>
</tr>
<tr>
<td>Few</td>
<td>53</td>
<td>78</td>
<td>57</td>
</tr>
<tr>
<td>A lot</td>
<td>52</td>
<td>77</td>
<td>59</td>
</tr>
<tr>
<td>SS No</td>
<td>57(^b)</td>
<td>83(^c)</td>
<td>65(^b)</td>
</tr>
<tr>
<td>Low</td>
<td>48</td>
<td>87</td>
<td>66</td>
</tr>
<tr>
<td>High</td>
<td>50</td>
<td>66</td>
<td>49</td>
</tr>
<tr>
<td>OA Low</td>
<td>56</td>
<td>78(^b)</td>
<td>52</td>
</tr>
<tr>
<td>Medium</td>
<td>55</td>
<td>80</td>
<td>61</td>
</tr>
<tr>
<td>High</td>
<td>50</td>
<td>71</td>
<td>58</td>
</tr>
<tr>
<td>f/v upset</td>
<td>63(^c)</td>
<td>88(^c)</td>
<td>69(^c)</td>
</tr>
<tr>
<td>n/b upset</td>
<td>47</td>
<td>65</td>
<td>54</td>
</tr>
<tr>
<td>Got over it</td>
<td>48(^b)</td>
<td>67(^c)</td>
<td>55(^c)</td>
</tr>
<tr>
<td>Lasted longer</td>
<td>60</td>
<td>85</td>
<td>72</td>
</tr>
<tr>
<td>TOTAL</td>
<td>53</td>
<td>77</td>
<td>60</td>
</tr>
</tbody>
</table>

\(^a\) = p<.05; \(^b\) = p<.01; \(^c\) = p<.001


f/v upset: very/fairly upset; n/b upset: not/a bit upset; got over it: got over it straight away; lasted longer: upset for at least a couple of days.

The number of children (bothered by) meeting online contacts was too low to conduct valid \(X^2\)-analyses on coping strategies.
### Table 2. Variables Predicting an Internet-specific Proactive Approach based on All Children who Have Been Bothered after Being Exposed to the Respective Online Risk in the Past 12 Months (%)

<table>
<thead>
<tr>
<th>Proactive approach</th>
<th>Delete message</th>
<th>Block sender</th>
<th>Try to fix the problem</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sexual Images Bullying Sexting</td>
<td>Sexual Images Bullying Sexting</td>
<td>Sexual Images Bullying Sexting</td>
</tr>
<tr>
<td></td>
<td>(n=971)</td>
<td>(n=1290)</td>
<td>(n=567)</td>
</tr>
<tr>
<td>Boys</td>
<td>25 39 33</td>
<td>24 43 33&lt;sup&gt;a&lt;/sup&gt;</td>
<td>25&lt;sup&gt;a&lt;/sup&gt; 30&lt;sup&gt;a&lt;/sup&gt; 23&lt;sup&gt;a&lt;/sup&gt;</td>
</tr>
<tr>
<td>Girls</td>
<td>26 43 41</td>
<td>22 48 45</td>
<td>19 41 29</td>
</tr>
<tr>
<td>Age 9-10</td>
<td>20&lt;sup&gt;b&lt;/sup&gt; 37 31&lt;sup&gt;b&lt;/sup&gt; 39&lt;sup&gt;b&lt;/sup&gt;</td>
<td>20&lt;sup&gt;b&lt;/sup&gt; 34&lt;sup&gt;b&lt;/sup&gt; NA</td>
<td>NA NA NA</td>
</tr>
<tr>
<td>11-12</td>
<td>21 43 31&lt;sup&gt;c&lt;/sup&gt; 31&lt;sup&gt;c&lt;/sup&gt;</td>
<td>26 43 45&lt;sup&gt;a&lt;/sup&gt;</td>
<td>23 27&lt;sup&gt;a&lt;/sup&gt; 35&lt;sup&gt;a&lt;/sup&gt;</td>
</tr>
<tr>
<td>13-14</td>
<td>32 42 34</td>
<td>17 50 30</td>
<td>22 43 21</td>
</tr>
<tr>
<td>15-16</td>
<td>25 40 44</td>
<td>28 47 46</td>
<td>21 36 27</td>
</tr>
<tr>
<td>SES Low</td>
<td>39&lt;sup&gt;c&lt;/sup&gt; 52&lt;sup&gt;c&lt;/sup&gt; 41</td>
<td>31&lt;sup&gt;c&lt;/sup&gt; 52 43</td>
<td>26 47&lt;sup&gt;c&lt;/sup&gt; 26&lt;sup&gt;b&lt;/sup&gt;</td>
</tr>
<tr>
<td>Medium Low</td>
<td>24 38 33</td>
<td>22 44 36</td>
<td>23 34 21</td>
</tr>
<tr>
<td>SES Medium Low</td>
<td>32 52&lt;sup&gt;c&lt;/sup&gt; 28</td>
<td>32 37 37</td>
<td>18&lt;sup&gt;a&lt;/sup&gt; 41&lt;sup&gt;c&lt;/sup&gt; 10&lt;sup&gt;b&lt;/sup&gt;</td>
</tr>
<tr>
<td>Medium High</td>
<td>25 44 40</td>
<td>21 46 38</td>
<td>19 29 26</td>
</tr>
<tr>
<td>High</td>
<td>25 36 36</td>
<td>23 47 44</td>
<td>26 44 32</td>
</tr>
<tr>
<td>EP No</td>
<td>32&lt;sup&gt;a&lt;/sup&gt; 46&lt;sup&gt;a&lt;/sup&gt; 37&lt;sup&gt;a&lt;/sup&gt;</td>
<td>19 48 49&lt;sup&gt;a&lt;/sup&gt;</td>
<td>19&lt;sup&gt;a&lt;/sup&gt; 29 34</td>
</tr>
<tr>
<td>Few</td>
<td>20 30 51</td>
<td>21 43 45</td>
<td>11 35 22</td>
</tr>
<tr>
<td>A lot</td>
<td>27 47 39</td>
<td>25 47 35</td>
<td>30 39 27</td>
</tr>
<tr>
<td>SS Low</td>
<td>27 43 37</td>
<td>20 49&lt;sup&gt;a&lt;/sup&gt; 39</td>
<td>18&lt;sup&gt;c&lt;/sup&gt; 37 26</td>
</tr>
<tr>
<td>Low</td>
<td>23 40 47</td>
<td>25 38 44</td>
<td>16 36 23</td>
</tr>
<tr>
<td>High</td>
<td>25 40 35</td>
<td>25 45 42</td>
<td>29 36 31</td>
</tr>
<tr>
<td>OA Low</td>
<td>23&lt;sup&gt;c&lt;/sup&gt; 38 10&lt;sup&gt;c&lt;/sup&gt;</td>
<td>12&lt;sup&gt;c&lt;/sup&gt; 33&lt;sup&gt;a&lt;/sup&gt; 10&lt;sup&gt;c&lt;/sup&gt;</td>
<td>13&lt;sup&gt;a&lt;/sup&gt; 34 12&lt;sup&gt;c&lt;/sup&gt;</td>
</tr>
<tr>
<td>Medium Low</td>
<td>20 43 37</td>
<td>22 46 43</td>
<td>21 37 23</td>
</tr>
<tr>
<td>High</td>
<td>36 39 44</td>
<td>29 48 42</td>
<td>26 36 35</td>
</tr>
<tr>
<td>f/v upset</td>
<td>29&lt;sup&gt;a&lt;/sup&gt; 46&lt;sup&gt;a&lt;/sup&gt; 40</td>
<td>27&lt;sup&gt;a&lt;/sup&gt; 49&lt;sup&gt;a&lt;/sup&gt; 39</td>
<td>30&lt;sup&gt;c&lt;/sup&gt; 46&lt;sup&gt;c&lt;/sup&gt; 31&lt;sup&gt;a&lt;/sup&gt;</td>
</tr>
<tr>
<td>n/b upset</td>
<td>23 34 37</td>
<td>19 40 43</td>
<td>15 26 23</td>
</tr>
<tr>
<td>Got over it</td>
<td>32&lt;sup&gt;a&lt;/sup&gt; 37&lt;sup&gt;a&lt;/sup&gt; 39</td>
<td>26 46 46&lt;sup&gt;a&lt;/sup&gt;</td>
<td>14&lt;sup&gt;c&lt;/sup&gt; 24&lt;sup&gt;c&lt;/sup&gt; 27</td>
</tr>
<tr>
<td>Lasted longer</td>
<td>21 46 38</td>
<td>21 50 35</td>
<td>35 44 30</td>
</tr>
<tr>
<td>TOTAL</td>
<td>26 41 38</td>
<td>23 46 40</td>
<td>22 36 27</td>
</tr>
</tbody>
</table>

Note: X²-test; <sup>a</sup>p<.05, <sup>b</sup>p<.01, <sup>c</sup>p<.001

**Fatalistic Approach**

Third, a child may also respond in a passive, rather fatalistic way: i.e. simply hoping that the problem would go away, or stop using the internet for a while. Children hoping that the problem will go away may believe that being bothered or harmed is only temporary and will not cause substantial or long-term harm.
As to sexual images, about one in four of those feeling bothered hope the problem will go away or stop using the internet. At a younger age, children

### Table 3.

Variables Predicting a Fatalistic Approach based on All Children Who Have Been Bothered after Being Exposed to the Respective Online Risk in the Past 12 Months (%)

<table>
<thead>
<tr>
<th></th>
<th>Stop using the internet</th>
<th></th>
<th>Hope the problem goes away</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Sexual Images Bullying Sexting</td>
<td>Sexual Images Bullying Sexting</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(n=971) (n=1290) (n=567)</td>
<td>(n=854) (n=1177) (n=524)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Boys</td>
<td>19 13</td>
<td>18</td>
<td></td>
<td>36</td>
</tr>
<tr>
<td>Girls</td>
<td>20 21</td>
<td>28</td>
<td></td>
<td>14</td>
</tr>
<tr>
<td>Age 9-10</td>
<td>50</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>11-12</td>
<td>21</td>
<td>14</td>
<td>33</td>
<td>23</td>
</tr>
<tr>
<td>13-14</td>
<td>21</td>
<td>16</td>
<td>26</td>
<td>21</td>
</tr>
<tr>
<td>15-16</td>
<td>21</td>
<td>14</td>
<td>21</td>
<td>26</td>
</tr>
<tr>
<td>SES Low</td>
<td>37</td>
<td>22</td>
<td>17</td>
<td>25</td>
</tr>
<tr>
<td>Medium</td>
<td>24</td>
<td>14</td>
<td>28</td>
<td>25</td>
</tr>
<tr>
<td>High</td>
<td>17</td>
<td>19</td>
<td>32</td>
<td>21</td>
</tr>
<tr>
<td>SE Low</td>
<td>26</td>
<td>33</td>
<td>35</td>
<td>20</td>
</tr>
<tr>
<td>Medium</td>
<td>25</td>
<td>21</td>
<td>23</td>
<td>31</td>
</tr>
<tr>
<td>High</td>
<td>26</td>
<td>11</td>
<td>26</td>
<td>16</td>
</tr>
<tr>
<td>EP No</td>
<td>25</td>
<td>24</td>
<td>25</td>
<td>10</td>
</tr>
<tr>
<td>Few</td>
<td>21</td>
<td>12</td>
<td>32</td>
<td>18</td>
</tr>
<tr>
<td>A lot</td>
<td>28</td>
<td>20</td>
<td>21</td>
<td>31</td>
</tr>
<tr>
<td>SS No</td>
<td>25</td>
<td>10</td>
<td>31</td>
<td>23</td>
</tr>
<tr>
<td>Low</td>
<td>22</td>
<td>27</td>
<td>18</td>
<td>39</td>
</tr>
<tr>
<td>High</td>
<td>28</td>
<td>25</td>
<td>22</td>
<td>20</td>
</tr>
<tr>
<td>OA Low</td>
<td>44</td>
<td>28</td>
<td>23</td>
<td>26</td>
</tr>
<tr>
<td>Medium</td>
<td>25</td>
<td>18</td>
<td>25</td>
<td>24</td>
</tr>
<tr>
<td>High</td>
<td>16</td>
<td>14</td>
<td>27</td>
<td>23</td>
</tr>
<tr>
<td>f/v upset</td>
<td>37</td>
<td>22</td>
<td>31</td>
<td>30</td>
</tr>
<tr>
<td>n/b upset</td>
<td>16</td>
<td>12</td>
<td>23</td>
<td>18</td>
</tr>
<tr>
<td>Got over it</td>
<td>19</td>
<td>11</td>
<td>23</td>
<td>18</td>
</tr>
<tr>
<td>Lasted longer</td>
<td>25</td>
<td>22</td>
<td>32</td>
<td>27</td>
</tr>
<tr>
<td>TOTAL</td>
<td>25</td>
<td>20</td>
<td>24</td>
<td>22</td>
</tr>
</tbody>
</table>

Note: X²-test: \( a=p<.05, b=p<.01, c=p<.001 \)
f/v upset: very/fairly upset; n/b upset: not/a bit upset; got over it: got over it straight away; lasted longer: upset for at least a couple of days.
The number of children (bothered by) meeting online contacts was too low to conduct valid X²-analyses on coping strategies.
are more likely to react in a fatalistic way. Boys and children from higher-class families seem to care less about encountering unwelcome sexual images, as they more often simply hope the problem would go away. When receiving an unwelcome sexual message, 22% do not undertake anything at all, and 18% stop using the internet. Boys are more likely to do nothing, waiting until the problem goes away while girls tend to go offline for a while. Also children with little self-confidence and those who feel harmed more intensely are more likely to stop using the internet. Surprisingly, this strategy is also more common among older children. One in four victims of online bullying hope the problem goes away and one in five interrupt internet use. Emotionally troubled children and those feeling more upset and for longer periods are more likely to respond fatalistically. Girls more often simply hope the problem will disappear without intervention. Overall, we see that children feeling seriously disturbed are more likely to go offline for a while. As to sexual risks, girls more often turn away from the computer, while boys seem to care less and simply hope the problem will go away.

Effectiveness of Coping Strategies:
Which Strategies Help Most in Coping with Risk?
In sum, what coping trends are emerging? The majority of the children feeling bothered by online risks will talk about it with somebody, mostly their peers or parents. This might indicate that awareness raising campaigns emphasizing communicative coping strategies have some impact. Communicative strategies are broadly adopted by members of socio-demographic groups identified as ‘low self-mediators’ (girls, younger children, lower SES children). Children with emotional problems or low self-efficacy are not more likely to talk about their negative experiences than children without psychological issues. More efforts could be made to encourage these low self-mediators to talk about their negative online experience with somebody they trust. Given the importance of the peer group in a teenager’s life, sharing this experience with friends can be helpful.
Yet, in some situations, especially in the case of serious or long-lasting harm, it could be useful to talk to an adult or look for professional help. Hence, for young people facing peer or conduct problems, and therefore perhaps less able to rely on friends or family, it is important to be aware of the possibility of talking with teachers and professional childcare workers when something has upset them.

A proactive approach is effective in preventing further exposure and harm, and increases young people’s coping capacity. Therefore it should be promoted as a favourable strategy. As the feeling of being upset intensifies, children’s tendency to proactively try to fix the problem also increases. Although proac-
tiveness is not limited to the more resilient groups, the willingness to tackle the problem is definitely stronger among those children with higher self-efficacy. This suggests that self-confidence is paramount for building up resilience. A proactive attitude is measured by asking whether the child will ‘try to fix the problem’ or not. This is a very general answer and could technically also involve illegal options or actions that violate other people’s privacy. Therefore, it is useful to take a look at some internet-specific coping strategies, i.e. deleting the message or blocking the sender.

These online coping strategies evidently require a certain level of digital skill. Hence, as expected, children’s overall internet competences are positively related to undertaking these actions. With a perceived success rate of about 80%, deleting messages and blocking the sender prove to be very effective strategies when confronted with sexting issues. Being a victim of online bullying, blocking the sender is obviously more effective (78%) than simply deleting the message (58%). In case of unpleasant experiences with sexual images, it seems more helpful to delete the content (82%) than to block the source or sender (71%). Obviously the strategy adopted depends on the risk at stake: when it comes to online bullying (a contact risk), the sender intends to repeatedly send nasty or hurtful messages to a specific person, while the number of senders is rather limited. Seeing unpleasant sexual images is a content risk, often from an anonymous source (spam, pop-ups) without an obvious intention to hurt a specific person.

To stop using the internet may prevent further exposure to unwelcome sexual content, but also entails missing online opportunities and thus, building up resilience capacity. Therefore, it can be considered the strategy one should least encourage. In sum, children acting as low self-mediators, due to socio-demographics and/or psychological problems, are more likely to use a strategy that may reduce their resilience capacities and online opportunities even more. Nevertheless, about seven in ten children going offline for a while after an upsetting experience indicate this strategy was ‘helpful’ to them, yet it is important to realize that ‘helpful’ in this case refers to the absence of further exposure to online risks. Especially when dealing with sexual images (77%), victims perceive that to stop using the internet is helpful. The most passive response – simply hoping the problem would go away – is quite common, and less related to specific socio-demographic or psychological characteristics.

In Context: From Empirical Evidence Towards Targeted Policy Development

While different European cultures share the tension between protectionism and children’s rights when it comes to presumed harm to minors, their substantive understandings of harm vary considerably. These cultural differences suggest
that we really know very little about how sexual (or violent, or other) content may affect any individual young person, and that policy initiatives whose articulated justification is the protection of minors, serve symbolic purposes and are rarely met with political resistance. What, then, is the actual basis for the harm-to-minors assumption (regarding sexual or other controversial content)? Answers range from the broadly moral (children must not be ‘robbed of their innocence’) to the developmental (anxiety, oversexualized behaviour), to the specifically imitative (children will mimic a certain activity). However, perhaps there are better ways to socialize children – such as training in media literacy and critical thinking, comprehensive sexuality education, literature classes that deal with difficult topics, inclusion of young people in journalism and policymaking. In all of these areas, economically and educationally deprived youngsters are likely to benefit most from additional sources of information and ideas (Heins 2001[2007]).

Public debates about the impact of new digital technologies echo earlier anxieties and their perceived positive or harmful potential for minors; from the early days of cinema, to the invention of the printing press, these forms were seen to carry a significant power for learning, while at the same time deemed harmful to those considered vulnerable. Screen-based media and other new technologies have raised public concern for various reasons in the past few years (e.g., seen as reinforcing traditional stereotypes and negative role models, as with gaming; as having a tendency to corrupt the young via the availability of online pornography; as causing imitative violence, or as hosting potential paedophiles who lurk online seeking to lure unsuspecting children); sometimes this concern is expressed in the call for stricter legislation, other times it leads to the view that parents and teachers should exercise greater control in order to prevent children experiencing such corrupting influences (Buckingham 2002). However, the debate about media regulation and parental mediation needs to be seen as part of a wider scheme wherein the relationships of power and authority between adults and children are changing as a result of the way in which the (new) media have been embedded within children’s everyday lives. We need to contextualize children’s uses of new technologies in relation to broader social, economic and political forces, asking traditional questions about access, control and public culture (Buckingham 2004: 122).

EU Kids Online has proposed a threefold classification of the risks of harm to children from their online activities, distinguishing content risks (in which the child is positioned as recipient), contact risks (in which the child in some way unwillingly participates), and conduct risks (the child as actor). All of these risks have been largely discussed in policy circles and have led to multi-stakeholder initiatives. There is also considerable consensus on the clusters of risk factors that are associated with negative outcomes (e.g., Smith and Carlson 1997). Nevertheless, the nature of harm is not always clear, and the conditions within
which risk of harm turns into actual harm remain poorly defined. Challenging
issues here concern the meanings of risk factors for children or adolescents
and their reactions to the risks they are exposed to. Relevant questions in this
context are: When does the opportunity of going online turn into a source of
adversity provoking stress? And how effective are children’s coping responses
to the incidence of risk of harm?

Indicators for a healthy development in the building of coping approaches
towards online risks are digital skills, especially when using internet-specific
coping responses are involved, and self-efficacy, when it comes to adopting
a proactive coping approach. However, the impact of digital competences
and self-efficacy depends on the type of risk encountered and how risk is
experienced (i.e. intensity of being upset and how long this lasted). Emotional
problems may pose a threat in the development of online resilience. Children
experiencing difficulties offline are likely to be less resilient online or miss tak-
ing up online opportunities, while children showing resilience offline are also
more likely to develop an adequate response to an adverse online experience,
and continue taking up online opportunities. Children facing psychological
problems continue to be less involved in problem-solving strategies. More initia-
tives on online coping and resilience building with an emphasis on children’s
psychological characteristics would be useful, focusing on the importance of not
giving up on internet use but instead trying to cope with online risks through
proactive and communicative strategies.

EU Kids Online made it one of its objectives to provide systematic, cross-
national empirical evidence, showing that individual socio-demographic and
socio-psychological factors determine a child’s level of vulnerability: girls,
younger children, those with low self-efficacy and low digital literacy require
special attention. Younger children are found to be most at risk of harm and
are more likely to go offline when exposed to content perceived as harmful.
Girls are also more susceptible to the harmful effects of sexual risks and tend
to react fatalistically, a recurring trend that needs attention and should be re-
versed. However, girls are more talkative than boys, no matter what type of
risk they are confronted with, possibly because behaviours and feelings that
suggest vulnerability are less accepted among boys. As girls are more com-
municative, parents, teachers and peers they trust and talk to could be advised
to steer them towards problem-solving strategies. A similar approach could
be used with other vulnerable groups as talking about the problem is often
the first step in reaching a suitable solution. This highlights the importance of
open communication both at home and at school.

Wendy Stainton Rogers offers a useful view on the discourses that inform
policy and practice oriented to the more vulnerable groups of children which
we feel is pertinent for our discussion here (2004). The ‘needs’ discourse largely
informs our understanding of children in the Western world, and applies both
to adolescents and younger children; being profoundly influenced by various strands of psychology, it construes children not so much lacking and vulnerable as inherently ‘problematic’, and thus ‘in need’ of adult surveillance, mediation and control. In this sense, although the ‘children’s needs’ discourse means well, motivated by the desire to improve children’s welfare, by positioning children in terms of their needs, it sets an expectation that adults should view them in relation to these needs and try to meet them. In effect, such a discourse demands that we must provide ‘solutions’ for the ‘problems’ posed by children’s needs, and as a result, children themselves are turned into ‘problems’ that need ‘solving’ (Buckingham 2004: 130); at the same time, they incorporate a ‘harm warranting’ as adult intervention is premised upon the warrant that it is necessary in order to protect a child from harm. On the other hand, children’s worlds have changed profoundly as a result of this ‘harm warrant’: as the ‘children’s needs’ discourse can orient (and distort) policy measures towards specific needs only (i.e. prevention of encounters with sexual content) to the exclusion of other ‘needs’ (e.g., access to information, being held incommunicado against their will), it thus renders them invisible. On top of that, conceptualizing childhood in terms of ‘needs’ reflects a predominantly western view of children, which despite its progressive and enlightened lustre, remains a framework that carries latent assumptions about them and imposes the specifically western values regarding children’s needs enmeshed within developmental psychology.

Harm warranting predicated upon a developmental perspective of childhood thus imposes a particularly western world view on how we construe children’s needs. Crucially, it adopts the western prioritization of the individual self, and of individual autonomy and freedom. Viewing the child as in transit towards becoming an autonomous, independent individual focuses our attention on what children ‘need’ in order to achieve this goal. But what if a different sort of adulthood is aspired to – one that values connectedness, mutuality and interdependence? (Stainton Rogers 2004: 132).

The previous discourse was countered by a move towards a ‘children’s rights’ discourse that was prevalent in the 1970s, whereby children were treated as social actors in their own right, capable of and entitled to have a say about what is done to and for them (James and Prout 1997; James, et al. 1998; Woodhead 1997). According to this discourse, children cannot be treated as ‘lesser mortals’, not deserving the same rights and respect as adults, just because they are not adults; within a ‘children’s rights’ approach, then, the intention would be to devise and deliver policies and services for them in ways that promote and safeguard these rights. However, this discourse is not immune to being appropriated by adults for their own purposes – parents are not saints; they get angry and out of line, they have divided loyalties and lose their temper, they are wrong. Professionals, too, may have their own battles to fight and some-
times may justify self-serving actions while claiming they are ‘in the child’s best interests’. Hence, when talking about children’s rights and policy initiatives to safeguard them, we need to bear in mind that adults do not always know best and may not always act in the most honourable ways, and that there must be some limits on adult power over children (Stainton Rogers 2004: 137).

In order to move beyond the ethnocentrism of the ‘needs’ and ‘rights’ discourses, argues Stainton Rogers, the ‘children’s quality of life’ alternative has been offered, which allows for a contextual understanding of children’s welfare as it acknowledges that the latter must take into account the concerns, values, resources and limitations of the families and societies in which children are reared and cared for. Such a discourse is premised upon the understanding that policy initiatives based on children’s rights (especially protection and provision of services) may be an improvement upon those based on children’s needs, though, it is still preoccupied with problems children face in adverse circumstances. Inevitably, it leads to an approach of identifying ‘risk factors’ (a situation wherein children need adults to intervene and redress the disadvantages they face, and protect them from harm). The alternative dictates that we turn away from what harms children and focus on what we can do to help them overcome difficulties and thrive in adversity – resilience being the key concept here. By nurturing children’s resilience, we go beyond merely meeting their (developmental) ‘needs’ and fostering their ‘rights’ – we help them flourish and achieve their life goals. In order to do so, we have to consult them and involve them in the plans and decisions to be made (Stainton Rogers 2004). Crucially, by focusing on the notion of the quality of life, we steer away from ‘problematizing’ children. Instead, looking at a child’s life experience, circumstances, values and priorities as a whole, we recognize that there is considerable variation in what is important to a particular child (alongside the families and cultures within which they live) and we are thus more respectful of social, cultural and religious variation. For some, this line of argument is bound to be more effective from a policy point of view (Stainton Rogers 2004: 143), as attempts to reduce the ‘risk factors’ that make children vulnerable have been unsuccessful, for they may stigmatize them and exacerbate social exclusion.

Instead, shifting the emphasis to how online resilience can be actively promoted may prove more fruitful in helping to target policy where it can enable even the most disenfranchised families to better understand the meanings of online risk factors that lead to harm as experienced by their children, and as such considerably improve their children’s quality of life. In that respect, we would argue, that concentrating on enhancing children’s capabilities – their resilience, so that they may counteract disadvantages and overcome adversity – would also mean policy initiatives that apply to all children, and not merely those at risk of harm. Focusing on the notion of quality of life allows us to transgress the ‘problematizing’ of children and their families as we search for the positive
qualities that (most) families may possess (such as good relationships, emotional warmth, support in times of crisis) – even the poorest and the most deprived. In addition, and given recent EU Kids Online findings (EU Kids Online 2011) whereby increased media literacy is coupled with increased chances of risky experiences, policy should aim for harm reduction, rather than risk reduction, through the development of coping strategies that build children’s resilience. The underlying rationale is that we do not wish to remove risk altogether from children lives, since not all risk results in harm as we have discussed above, and because such action would needlessly jeopardise children’s online opportunities as well; what we should be aiming at, instead, is to promote policy initiatives that consolidate children’s coping strategies so that their experience of harm is reduced while their resilience is not compromised.

Notes

1. The concept of self-efficacy consists of four items: ‘I am confident that I can deal with unexpected problems’, ‘It’s easy for me to stick to my aims and achieve my goals’, ‘If I am in trouble I can usually think of something to do’, ‘I can generally work out how to handle new situations’ (Cronbach’s alpha=.68). Sensation seeking is measured by two questions: ‘I do dangerous things for fun’ and ‘I do exciting things, even if they are dangerous’ (Cronbach’s alpha=.79). Emotional problems is a concept resulting from the following five items: ‘I get a lot of headaches, stomach-aches or sickness’, ‘I worry a lot’, ‘I am often unhappy, sad or tearful’, ‘I am nervous in new situations, I easily lose confidence’ and ‘I have many fears, and I am easily scared’ (Cronbach’s alpha=.68).

2. Online activities: list of 17 online activities (information, entertainment, communication and creative uses).

References


Chapter 14

Protection versus Privacy

An Area of Conflict

Andrea Duerager, Sonja Duerager & Ingrid Paus-Hasebrink

Recognizing that the child, for the full and harmonious development of his or her personality, should grow up in a family environment, in an atmosphere of happiness, love and understanding, ...


The internet plays an important role in the daily lives of young people. It fulfils several functions in identity management, social management and information management (Paus-Hasebrink, Lampert, Hasebrink 2009). For most children and adolescents, using media and the internet to deal with the challenges of growing up is an important part of their development. Thinking about children's opportunities in this context also requires us to consider the risks they may face. Looking back on more than 20 years of the UN Convention on the Rights of the Child (UNCRC 1989), we have to remember that the Convention includes the right to “development of the child's personality, talents and mental and physical abilities to their fullest potential” (article 29) (see OHCHR 1989; Hammarberg 1990: 97). This, as the Convention makes clear, also refers to children's media use and encourages that “information and material of social and cultural benefit to the child” is disseminated, as media are a central part of children's everyday lives (article 17). To guarantee this, a balance is required between protecting children's need for and right to privacy on the one hand and protecting them from risks and harm on the other hand. Yet this often raises conflicts. This chapter focuses on ‘privacy’ as one issue within the broader discourse on internet safety. We examine privacy-related risks and different perspectives on how to protect children against negative or harmful experiences. Firstly, we provide empirical evidence from the EU Kids Online survey about online risks regarding privacy and experiences with potentially harmful online content. Secondly, we discuss different options to protect children specifically social mediation and legislation. The final part considers possible contributions of stakeholders to protecting children’s online privacy and safety.
Exposure to Private Data and Inappropriate Internet Content

The aim of the internet safety policy emanating from the European Commission (EC) is to ensure that children enjoy online opportunities “without worrying about threats to their [the users’] privacy or viewing inappropriate content” (European Commission 2012). Even though an internet so safe that nobody has to worry about negative online experiences anymore may be unattainable, there is undoubtedly a need to make it safer, especially for children. As a certain amount of risk always remains, awareness raising for possible threats through media education is essential for keeping online experiences as positive as possible. Yet, children continue to encounter risk through threats to their privacy and exposure to inappropriate content. In this chapter, we focus on two aspects of privacy in online activity: (1) the use of social networking sites (SNS) including risks to privacy, and (2) the entitlement to privacy when using the internet including the danger of being exposed to inappropriate content.

In general, negative online experiences can be classified in terms of children’s online activities. These are differentiated on the basis of the role the child plays within these activities: Content risks refer to the child as recipient, contact risks deal with the child participating – also unwillingly, in an action that is initiated by someone else and conduct risks see the child as an actor (see Table 1).

Table 1. Risks Relating to Children’s Internet Use (exemplars only)

<table>
<thead>
<tr>
<th></th>
<th>Content</th>
<th>Contact</th>
<th>Conduct</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Receiving mass-produced content</td>
<td>Participating in (adult-initiated) online activity</td>
<td>Perpetrator or victim in peer-to-peer exchange</td>
</tr>
<tr>
<td>Aggressive</td>
<td>Violent / gory content</td>
<td>Harassment, stalking</td>
<td>Bullying, hostile peer activity</td>
</tr>
<tr>
<td>Sexual</td>
<td>Pornographic content</td>
<td>‘Grooming’, sexual abuse or exploitation</td>
<td>Sexual harassment, ‘sexting’</td>
</tr>
<tr>
<td>Values</td>
<td>Racist / hateful content</td>
<td>Ideological persuasion</td>
<td>Potentially harmful user-generated content</td>
</tr>
<tr>
<td>Commercial</td>
<td>Embedded marketing</td>
<td>Personal data misuse</td>
<td>Gambling, copyright infringement</td>
</tr>
</tbody>
</table>


First, we want to focus on the careless exposure of private data, in particular through poorly applied privacy settings on social networking sites (SNS) that might lead to violation of the child’s privacy. In an age of fast growing internet communication through SNS services like Facebook or video sharing portals such as YouTube, making private information public has become very easy. According to EU Kids Online, 59% of European children aged 9 to 16, have
a social networking profile, the probability of having a SNS profile increasing with the child’s age. Out of these, 23% have more than one profile on a social networking service. Considering the continuing rise in popularity of social networking, we have to bear in mind that SNS “integrate online opportunities and risks more seamlessly than any other online service” (O’Neill, Livingstone and McLaughlin 2011: 24). In making private data public within SNS, several contact and conduct risks could occur: undesired identification of children which might especially lead to contact risks such as stalking, harassment, grooming, identity theft, unlawful selling of user database to third parties, spam and phishing. Likewise, users encounter conduct risks like cyber-bulling or sexting by making private information even (partly) publicly available (European Commission 2012) as e.g. “the possibility of tagging people in pictures, offered by most social networking services, makes it very easy to search for a person’s photos online” (European Commission 2011a).

Taking these possible risks into account, the fact that 26% have a public profile is alarming given that anyone registered on the service can access it unbeknownst to the profile owner. 28% of 9 to 16 year old children keep their profile partially private, meaning that friends of friends can also check them (30% have 11 to 50 so-called “friends”, 48% have 50 or more contacts). Only 43% keep their profile private, which means only friends can see what they do. On average, 3% do not know which settings they have; in the case of children aged 9 to 10, 9% responded that they did not know. As the default privacy settings on most SNS services are set to public or partially private (European Commission 2011a), these children also may not have private profiles. Profiles of children, the survey reveals, include the following information: a photo that shows their face (76%), their last name (64%), their address (11%), their phone number (7%), the name of their school (43%), their correct age (61%). Differences in displaying information are also apparent according to the privacy setting: users who have a public profile offer more information than those who keep their profile private (Figure 1).

Beyond that, one third of all children added people that they have never met face to face to their friends' list or address book. 15% of all children sent personal information (e.g. their full name, address or phone number) and 13% sent a photo or video of themselves to someone not known in person. There is a tendency for older children to provide more personal information and behave more carelessly than younger ones and that children who are more inattentive with their data are also more likely to find their information misused: e.g. 14% of those who displayed all six kinds of information in Figure 1 also stated that somebody used their password to access their information or pretended to be them. For those who did not share personal information, the finding was 7%.

Consequently, the need for protection of children's privacy is increasing. Preventing children from using SNS is unlikely to be effective or wise given the
Figure 1. Provision of Private Information Dependent on Profile Settings

Base: All children who use the internet and have a SNS profile.

The multitude of opportunities that social networking provides young people with. Hence, raising children’s awareness of privacy as something that should be protected as well as supporting “digital skills to protect privacy and personal data” (O’Neill, et al. 2011: 25) are the main actions to be taken. Equally important, as policy makers have been keen to point out, are the safety tools provided by SNS companies: “Youngsters do not fully understand the consequences of disclosing too much of their personal lives online. Education and parental guidance are necessary, but we need to back these up with protection until youngsters can make decisions based on full awareness of the consequences” (European Commission 2011a).

In addition to the disclosure of personal data and the consequent contact and conduct risks that arise, another aspect that assumes particular importance in relation to risks to children’s privacy is that of ‘hard to monitor’ websites such as so-called user generated sites containing potentially harmful content. Ideally, children should be able to avail themselves of all the opportunities that the internet offers, safe from the risk of being exposed to inappropriate content. Findings from EU Kids Online show that 21% have had contact with inappropriate websites: 7% saw websites that contained information about ways of physically harming or hurting themselves, about talking or sharing experiences of drug taking; 5% encountered sites which discussed ways of committing suicide; 10% accessed sites that included information about how to be very thin (such as being anorexic or bulimic); 12% viewed sites with hate messages that attack certain groups or individuals; and 14% accessed sites with sexual images.
Again, the older the children are, the more likely they are to come in contact with such websites. As illustrated in this chapter, the online activities children engage in and the information they disclose about themselves can result in both positive and negative experiences. Consequently, the more opportunities children use, the more risky online experiences they face ($r = .419$, $p < .05$). On the one hand we have to ask what can be done by caregivers such as parents, teacher or peers, as well as what kind of action can be taken by legislators or online service providers to enable children to enjoy various internet activities while, at the same time, avoiding online risks and harm. On the other hand, we have to respect children’s right to privacy; this right and the fact that children might even profit from online activities we call risky requires that we deal judiciously with measures restricting access to the internet. The following sections deal with these dilemmas.

Social Protection of Children’s Internet Use

What can be achieved within children’s social environment by parents, teachers or peers to foster online opportunities, to reduce negative experiences and to raise young people’s digital competence and their awareness of privacy issues as well as to sensibilise them to risks that may arise from online activities?

One of the main objectives of the European Union’s Safer Internet Programme$^1$ is to educate users in safer internet practices (European Commission 2012). Raising awareness of online risks “for children and young people, parents, carers, social workers and teachers to enable children and young people to make responsible use of online technologies” (European Commission 2011b) is one of the central aspects of this programme, promoting the careful handling of private data and online content. While parents, teachers, peers and others are expected to support children and young people in this regard, it is also something that requires digital skills on the part of young people. Consequently digital education on a broad level is needed.

The widely recognized concept of parental mediation, is valuable for parents to engage with their child’s internet use and employs a range of strategies according to the age of the child (O’Neill, et al. 2011: 36). According to Livingstone and Helsper (2008), five main strategies of parental mediation can be identified: active mediation of use, active mediation of safety, restrictive mediation, monitoring and technical mediation (Livingstone et al. 2011). Findings from EU Kids Online (Duerager and Livingstone 2012) show that restrictive mediation is the most effective of all parental mediation strategies in reducing risk and harm, though obviously it also reduces the number of online opportunities. Active mediation of children’s internet use – i.e. where parents talk to their children about the internet, stay nearby or sit with them while they go online – is asso-
associated with lower risk and lower harm, and is linked to more online activities and skills. There is evidence that active mediation of safety and monitoring are more likely to be used after a child has experienced something negative online to protect them from further problems. The results show that both strategies raise online opportunities and skills. Though monitoring would also appear to be effective, it is questionable from the point of view of the child’s privacy, involving intrusion, for instance, into children’s social networking profiles or checking websites the child has used. Finally, technical mediation has no significant impact though filtering and family protection software are widely promoted aspects of internet safety (Duerager and Livingstone 2012).

For sure there is evidence that parental mediation is able to influence the child’s online behaviour in a positive way – hence there is a need to inform parents more on this point, as “there are some parents who do not do very much, even for young children, and there are some children who wish their parents to take more interest. Targeting these parents with awareness raising messages and resources is thus a priority.” (O’Neill, et al. 2011: 35)

Apart from parents, teachers and peers have an important role within the mediation process, as well as third parties such as social workers. Concerning mediation actions of teachers and friends, correlations show that they lead to more online activities (teachers: \( r=0.096, \ p<0.05 \); peers: \( r=0.147, \ p<0.05 \) and also more digital competence (teachers: \( r=0.115, \ p<0.05 \); peers: \( r=0.104, \ p<0.05 \). But, there are also positive correlations with online risks (teachers: \( r=0.015, \ p<0.05 \); peers: \( r=0.089, \ p<0.05 \) and negative experiences that make respondents feel fairly or very upset (teacher 9-10: \( r=0.094, \ p<0.05 \); teacher 11-16: \( r=0.081, \ p<0.05 \); peers 9-10: \( r=0.217, \ p<0.05 \); peers 11-16: \( r=0.097, \ p<0.05 \). In both cases, again, the intervention with mediation strategies might be a consequence of risky experiences: when children come into contact with online risks or have negative experiences, teachers as well as peers might intervene through mediation actions to help those children. This result is undermined by the mean difference between children who say they have experienced something online that bothered them and those who have not (teacher: \( t(3527)=9.791, \ p<0.05 \); peers: \( t(23189)=11.127, \ p<0.05 \).

Finally, children were asked in the EU Kids Online survey if they ever received advice about how to use the internet safely from a number of listed people or institutions (see Table 2). Next to relatives, different kinds of media seem to be an important way for getting information, the relevance of which increases with the child’s age. The correlations show that children who get advice from third persons or institutions use more opportunities and become more internet literate. Moreover, children who experience more online risks might be more likely to search for advice in various places.
Mediation strategies and support by various persons and sources, but especially those closest to the social environment of the child (parents, relatives, peers, teachers and the school system as a whole), as well as public institutions like media companies and providers, are central to efforts for promoting online opportunities, fostering digital skills and literacy, raising children’s awareness of privacy and general online risks and enabling children to cope with negative online experiences. Still, it is essential that children, especially younger ones, who have not yet encountered risks or harm, also acquire skills and information relating to internet safety. Hence, preventative communication has to be boosted.

## Protection of Children’s Privacy Through Legislation

When investigating types of legal measures for protection of children in the online world that should exist, we have to consider fundamental human rights that determine the scope for any legal act granting or interfering with the freedom of citizens. Primarily, fundamental rights guarantee specific subjective rights for individuals. Within the scope of these rights, the state has to outlaw potential infringements, for instance, censorship of the press. However, fundamental rights are not just those related to repelling government actions; fundamental rights are deemed as objective basic norms for governmental action (Berka 1999: 50 et seq.). As a result, there are positive obligations on the state to realize the protection of individual freedom by legal acts. Such obligations may involve the adoption of measures designed to secure respect for private life, referring to relations between citizens and state, on the one hand, as well as relations between individuals on the other hand (ECHR 2004). Thus, the

### Table 2. Source of Advice Received about How to Use the Internet Safely Depending on Age [%]

<table>
<thead>
<tr>
<th>Person/Institution</th>
<th>9-10</th>
<th>11-12</th>
<th>13-14</th>
<th>15-16</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td>Youth or church or social worker</td>
<td>4.1%</td>
<td>5.1%</td>
<td>7.1%</td>
<td>7.7%</td>
<td>6.1%</td>
</tr>
<tr>
<td>Librarian</td>
<td>3.8%</td>
<td>6.4%</td>
<td>5.9%</td>
<td>5.7%</td>
<td>5.5%</td>
</tr>
<tr>
<td>Other relative (e.g. brother, sister, aunt, uncle, grandparent etc.)</td>
<td>45.2%</td>
<td>48.8%</td>
<td>48.9%</td>
<td>43.0%</td>
<td>46.5%</td>
</tr>
<tr>
<td>Someone whose job it is to give advice over the internet</td>
<td>4.8%</td>
<td>8.1%</td>
<td>10.9%</td>
<td>12.2%</td>
<td>9.2%</td>
</tr>
<tr>
<td>Websites</td>
<td>4.6%</td>
<td>9.0%</td>
<td>13.7%</td>
<td>20.2%</td>
<td>12.2%</td>
</tr>
<tr>
<td>Television, radio, newspapers or magazines</td>
<td>10.4%</td>
<td>19.4%</td>
<td>22.9%</td>
<td>24.9%</td>
<td>19.8%</td>
</tr>
<tr>
<td>Internet service provider i.e. the company that provides the internet to your home or school</td>
<td>2.7%</td>
<td>4.6%</td>
<td>7.7%</td>
<td>9.8%</td>
<td>6.4%</td>
</tr>
</tbody>
</table>

Base: All children that use the internet.
idea behind fundamental rights is that the state has to enable and guarantee that citizens live together in a spirit of peace, in freedom, equality and dignity (Berka 1999: 1 et seq.).

As the internet plays an increasingly central role in the private lives of children, the right to respect for private and family life\(^2\) assumes ever more importance in discussions about regulating access to the internet in order to protect infantile and adolescent users. The right to privacy guarantees that anyone can freely develop their personality through their contacts and interpersonal relationships, irrespective of whether they occur online or offline. This includes the principle of autonomy and the right to informational self-determination. Generally, there should be no interference by the state when exercising this right, as long as it is not necessary to protect the interests of the community. Hence, the state must abstain from restricting children’s internet use when communicating online or searching for information. However, the right to privacy requires that the state also takes measures in order to proactively protect children in their online behaviour against harmful influence, or intrusions on their privacy.

This dualism between free access and protection is articulated in the UN Convention of the Rights of the Child (UNCRC), Article 13 of which guarantees the right to freedom of expression and thereby the free access of children to information. Article 17 promotes the development of guidelines for the protection of children from information and material injurious to their well-being. Overall, the UNCRC offers a forceful statement of the obligation on governments to take adequate measures for the protection of children from hazardous information (Sommerauer 2009: 81).

Safe and free internet use by children is also a particular interest and priority of the European Union. Apart from a number of other legal acts for protecting children online, in 2006 the European Parliament issued a recommendation on the protection of minors including a number of measures with the specific objective of promoting a safer internet for children (e.g. a generic second level domain such as ‘.KID.eu’). Recently, the European Commission stated in a communication to the European Parliament that it aims to achieve a high level of protection of children in the digital space, including their personal data, while upholding their right to access the internet for the benefit of their social and cultural development (COM 2011). A central aspect of this is the Audiovisual Media Services Directive of 2010, which deals with on-demand audiovisual media services and requires Member States to take appropriate measures to ensure that services which might seriously impair children's physical, mental or moral development are only made available in such a way that minors will not normally hear or see them (Article 12 AVMSD). Finally, the intention of the Commission to substitute the current Data Protection Directive by a General Data Protection Regulation (GDPR) shall be emphasized. The first proposal of
this regulation as of 25/01/2012 expressly mentions the necessity to protect children’s data processed by online services.³

From all these abovementioned legal acts, it follows that, on the one hand, children have the right to freely access new media as part of their right to privacy without being restricted by the state. On the other hand, there are also obligations on the part of the state inherent in effective respect for private or family life and thus, governments have to encourage the development of appropriate guidelines for the protection of children from information and material injurious to their well-being. Thus, the state is at fault if it does not protect or seek to protect young people from content not suitable for them (ECHR 2005), in particular by an effective legal framework.

Now the challenge for states is to issue regulations, which include a fair balance between the general interest of the community in protecting children, and the competing interests in promoting and respecting children’s right to privacy (ECHR 1989), and hence, the right to free internet use. Hereinafter we present by way of example how Austria⁴ tries to deal with some of these issues and potential problems.

**Youth Protection in Austria**

*Harmful Content*

In Austria, the positive obligation of the state to protect minors in their use of new media with regard to harmful content is implemented on the basis of the federal Youth Protection Acts and on the Audiovisual Media Services Act (AMDG).

Austria has transposed the abovementioned AVMSD in the AMDG. It provides that access to on-demand audiovisual media services with content harmful for minors shall be restricted by the media service providers with adequate measures to control access. The act itself grants a wide discretion to media service providers, because only content which could impair children “seriously” requires access control. Furthermore the act fails to enumerate specific control measures (Section 39 AMDG). It must be emphasized that audiovisual media services are only services with a commercial purpose and thus any services distributing content for private purposes (e.g. a private website with holiday pictures) are exempt from the scope of this act (Kogler, Traimer and Truppe 2011: 413).

According to the Austrian Youth Protection Acts, it is forbidden to transfer, present or otherwise make accessible media that could be harmful for the development of children. This prohibition also applies to private websites. If someone offers such harmful media commercially, they are obliged to exclude minors from access to such media by adequate and effective measures. The wording “harmful to the development” is not defined conclusively. However, in particular,
but without limitation, violent and brutal content, actions which discriminate against human beings for whatever reason (e.g. their race or sex) or pornographic presentations, are deemed to be hazardous for minors (Sommerauer 2009). The term “harmful” does not obviously require a certain qualification, such as the notion “seriously”. However, the Youth Protection Acts fail to proclaim which precautions should be taken in order to prevent access by minors.

The question of which measures should be taken in order to guarantee that harmful content is only consumed by adults is a tricky one. Age verification systems are often discussed as appropriate and effective measures. The Article 29 Data Protection Working Group (2009a; hereinafter Art 29 Group) has already expressed that an age verification system should be standard for all websites with harmful content or on websites that need the consent of parents. The Austrian legislator communicates in the explanations to the AMDG that cryptographic techniques, smart-cards, PINs, passwords or any other age verification system could be appropriate access control measures (Government Bill, 2010). Mere cautionary notices, such as “the content is not for people under 18”, or an age check without revision are not deemed to be sufficient (Krammer 2007: 70), especially in the case of non-commercial websites (Sommerauer 2009). In order for providers to perform an age check, age verification on the basis of the disclosure of the ID number on a photo identification is required (e.g. Leitl and Mayrhofer 2004: 360). In Germany, the German Supreme Court (2007) has already qualified such verification systems as insufficient and hence requires identification by means of face-to-face contact for the first time (Krammer 2007: 68). Against this background, the “Postident” procedure in cooperation with the German postal service has to be mentioned (German Supreme Court 2007). The user has to register personally with a passport and is, therefore, identified in the offline world. After identification he receives his user data for the website. Such systems, introduced for the purposes of promoting the system of digital signatures, would probably be reliable, but are complex. Thus, it is rather unlikely that operators of websites with (potential) harmful content would implement such a system voluntarily.

Hence, arguably it is the task of the state to develop more sophisticated verification systems and to expressly prescribe them by law. It remains to be seen if the idea of a verifiable consent as laid down in the proposal of the GDPR pushes the discussion about effective age verification systems. Finally, it has to be pointed out that all these measures are normally not effective for social networks (Günter, Schindler 2006: 350) considering that the operator of a SNS does not himself offer the content and therefore does not need to take control measures. However, the operator is obliged to remove the content or to disable the access to the content without delay if he becomes aware of illegal activities or information. At that time, depending on the circumstances of the individual case (e.g. number of users, commercial or non-commercial
network), the operator could be made responsible for continuously monitoring the content of a website in order to prevent the repetition of such an infringement (Austrian Supreme Court 2006).

**Data Protection**

Another aspect of the right to privacy is the protection of personal data. The Data Protection Act (DSG) is the legal framework for the use of personal data, which is of particular interest for the admissibility of generating and processing data of children via new media tools. As we have learned, 59% of European children have profiles on SNS, which include photos, their name, address or age. All this information corresponds with the legal definition of personal data, including information relating to an identified or identifiable natural person. Notwithstanding that children disclose data without any need to do so and also without exerting influence over who can have access to the data, the operator of the SNS regularly collates online data together to generate more information about the user, and uses the information for its own purposes, *inter alia* for advertising (e.g. Facebook data use policy, 2012). In this way, the operator qualifies as a so-called controller under the DSG and is consequently bound by the restrictions of the DSG for processing data.

Generally speaking, the processing of data is only permitted under the principle of proportionality. Thus, the use of data must occur only within bona fide and legal ways for clearly defined purposes. Further, the purpose and content of the processing of data may not violate protected secrecy interests of the data subject. In this sense, the DSG mentions a number of reasons for justification for data processing, for example that the data subject has unambiguously given his consent, that processing is necessary in order to protect the vital interests of the data subject, and that processing is necessary for the purposes of the predominant legitimate interests pursued by the controller (e.g. processing is necessary for the performance of a contract to which the data subject is party).

In connection with SNS, the legal justification for the processing of data is normally the consent of the user (see also Leissler 2010: 834). Consent means any freely given, specific and informed indication of wishes by which the data subject signifies his agreement to personal data relating to him being processed. The consent declaration, therefore, has to contain the detailed description of the data application (used data, the purposes of processing, details of the data importer), and the special note that the data subject is entitled to revoke the consent at any time. The consent is only valid if the data subject is fully informed about the prevalent circumstances, and this can naturally only be affirmed if the information is complete, correct and understandable as such (Leissler 2010: 834 *et seq.*). The Art 29 Group (2009a) lists information about
usage of the data for direct marketing purposes, about possible sharing of the data, and an overview on profiles as examples.

In particular, with a view to the structure of consent declarations on SNS (e.g. in several cases not one comprehensive declaration, but a number of accompanying texts that are linked to each other) and to the fact that the processed data are often extended by new applications without separate notification to the users, the argument could be brought that such consent declarations do not comply with the aforementioned requirements. However, even if the information was understandable for adults, minors could not comprehend it. This begs the question as to whether minors are able to give valid consent with regard to the respective data application for the SNS. In Austria, it is not the legal capacity of the minor, depending on the age, but the capacity to understand that is decisive. So, the child or adolescent data subject must understand the facts and must be able to assess the future consequences of such data processing (Jahnel 2010: 182).

Considering that for the SNS operator, it is hardly possible to ascertain the mental abilities of the user, it would be advisable to require the consent of the parents for any minor user (see also Art 29 Group, 2009a, 14). The Art 29 Group (2009b) has already stated that children’s consent must be provided by their parents before collecting and further using children’s data for the purposes of engaging in behavioural targeting of children. Also the proposal for the GDPR prescribes that the processing of data of a child below the age of 13 years shall only be lawful with the consent of the parents (Article 8). Hence, only in the context where minors are excluded from online advertising measures or any other act of processing data, should there be a margin of discretion not to require the consent of the parents.

Discussion and Conclusion

A look at the world media landscape for children and youth immediately presents two opposing themes: opportunities and risks. For example, globalization of media brings opportunities to broaden children’s perspectives and provide more equal access to information, but it also threatens cultural identification and values. Technological advances bring the promise of new skills and greater youth participation in society, but also increase the risk of child exploitation and informational divides. There is an urgent need for societies to both protect youth and empower them to shape their own media environments, as spelled out by the United Nations Convention on the Rights of the Child and increasingly by media experts and educators around the globe. (UNICEF 2004)

This diagnosis of the United Nations gets to the heart of the situation. The dilemmas that we face when trying to protect children from negative online experiences are: (1) that we might reduce opportunities simultaneously by re-
ducing the chance to encounter risks (2) that risks are not negative per se, they can also have positive consequences and (3) that we might violate the child’s privacy, for instance by regulating specific online content through legislation or by monitoring the child’s internet use through parents.

In order to be able to realize the above mentioned aspects, it is necessary to take the three principles of provision, participation and protection rights, as articulated in the UNCRC, seriously and put them into practice. With regard to forms of ‘protection’ that do not limit children’s opportunities, this chapter argues that a paradigm shift is needed. Protection can only be successful if everybody works together on solutions – children, parents, politicians and industry, as well as schools, teachers and peers. But if not taken seriously, a multi-stakeholder approach means nobody feels responsible.

With regard to the protection of privacy, it is essential to increase the awareness of privacy among children. Moreover, a major step towards greater protection and more privacy for children would be privacy settings that are set to private by default. Further, providers could meet obligations to better guarantee the protection of minors. The first step in this direction is the obligation of providers to control the access of minors to harmful content by appropriate measures. However, this obligation is not applicable to host providers in relation to their users’ content. A good starting point for this industry are the “Safer Social Networking Principles”, developed by providers of SNS in consultation with the EC, to enhance the safety of children and young people using their services, to which 21 companies, to date, have committed (European Commission 2009). The protection of personal data of minors, as one important aspect of the right to respect privacy, could be realized more effectively by the consent of parents. The practical problem of how providers can effectively verify the age of users remains, though.

Following the recommendations of EU Kids Online, provision of appropriate positive online content, particularly for younger children, should be a priority; “the ‘European Award for Best Children’s Online Content’ is a valuable step in this direction, but such provision could also be supported by high profile national initiatives” (O’Neill, et al. 2011: 22). Other stakeholders such as the media can also make a contribution to a safer internet in terms of privacy protection, especially by providing public information that raises awareness of online risks. As far as parents’ responsibility is concerned, they could, for example, use age verification systems supported by browsers in order to make the internet safer for their children; this system must be easy to use for parents – and not easily hacked by children. Filter programs can support parents’ mediation strategies, but they cannot be the only solution. In particular, parents but also teachers are asked to effectively teach especially younger children responsible handling of social media and the internet itself, and to make internet use and safety a relevant topic in everyday life.
Notes


2. Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and Article 7 of the Charter of Fundamental Rights of the European Union

3. The GDPR is still subject to the decision-making process (http://ec.europa.eu/prelex/dtail_dossier_real.cfm?CL=en&DosId=201286, 14 October 2012)

4. We chose Austria as legislation is very specific in each country, and Austria is the example best known to the authors.

References


AVMSD, Directive 2010/13/EU of the European Parliament and of the council on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services.


Chapter 15

The Cultural Context of Risk

On the Role of Intercultural Differences for Safer Internet Issues

Uwe Hasebrink & Bojana Lobe

Children’s patterns of internet use as well as the risks they encounter and the harm they experience are substantially shaped by cultural contexts. While this statement may be commonly accepted, its conceptual and empirical basis is rather vague. What do we mean by cultural context? How exactly does this context “shape” which kinds of practices and experiences? Addressing such questions is particularly important when it comes to policy recommendations, which aim at increasing internet safety on a European level: in this case we need some evidence on which recommendations are likely to be helpful throughout Europe, and which recommendations will only be helpful within particular cultural contexts. However, so far comparative research has not yet reached a position that would allow for ‘culture-tailored’ policy recommendations. The epistemological, methodological, and theoretical problems of intercultural comparisons are too diverse (Jowell 1998). Comparative research is also politically sensitive; it defies the idea of common and united European approaches and therefore many of the principles underlying EU affairs. The EU Kids Online network aimed to solve some of these problems and to contribute some progress to this kind of research. This has partly been realised by providing rich empirical evidence on country differences and similarities within Europe – by means of a synopsis of previous research (Hasebrink, et al. 2009) and by means of a comprehensive comparative survey in 25 European countries (Livingstone, Haddon, Görzig and Ólafsson 2011; Lobe, et al. 2011). This empirical evidence has been used as a base for policy recommendations regarding promotion of internet safety (O’Neill, et al. 2011; O’Neill and Staksrud 2012).

With this as a starting point, this chapter discusses the opportunities and limitations of comparative research and tries to understand in which respect cultural contexts shape children’s experiences of risk and harm and thus require culture-specific approaches in order to promote internet safety. In the following, we discuss:
• What kind of empirical evidence can comparative research provide for the development of policy recommendations?

• Which particular differences within Europe can be observed with regard to children’s online practices, experiences of risk and harm, and parental mediation?

• Which kind of evidence can be used to classify European countries according to the cultural context they provide for children’s online experiences?

• What are the consequences for the development of policy recommendations on a European level?

Types of Comparative Research and Their Relevance for the Policy Process

In an often-quoted typology of comparative research, Kohn (1989, see also Livingstone 2003, and Hasebrink 2012) distinguished four approaches to cross-country comparisons: 1) countries as objects of study, 2) countries as a context of study, 3) countries as a unit of analysis, and 4) countries as part of a larger international/global system. Each of these four options will be discussed with regard to the kind of empirical evidence they provide as well as to their function in the policy process. The argument here is that each form of comparative research, understood as a specific form to consider cultural contexts, fulfils a specific role within the process of safer internet policy.

Widening the Horizon of Options

The first option within Kohn’s classifications, the “countries as objects of study” approach, refers to studies that are not comparative in a more ambitious sense but just provide reports about single countries. This kind of evidence can be both helpful and stimulating within a policy process. A characteristic of cultural contexts is that people within that environment regard any phenomena that occur as quite normal. Cultural context frames the range of patterns of behaviour, of attitudes towards children and risky experiences, and of strategies to prevent children from harmful experiences, that are perceived as ‘normal’ and acceptable. This type of comparative research, which provides reports on the specific experiences in other countries, can widen the horizon of alternatives by demonstrating different patterns of online use or parental mediation and different approaches to regulating online content.
**Enhancing the Knowledge Base**

The main objective of Kohn’s “countries as a context of study” option of comparative research is to test universal hypotheses across a sample of countries (see Figure 1; Hasebrink 2012). In each country the respective research investigates correlations between a theoretically defined set of variables, and then compares the extent to which these correlations and the fit of the overall model are the same for all countries. An example would be research on the question of how age (V1) and gender (V2) on the one hand, and the socio-economic status of the household (V3) and the type of parental mediation (V4) on the other, influence the likelihood of children having negative experiences on the internet (V5).

**Figure 1.** Logic of the “Countries as Contexts of Study” Approach

With regard to policy making, this approach to the analysis of behaviour and experience in different cultural contexts can enhance the knowledge base. On the one hand, this is obviously true for countries where no data on a concrete issue is available; in these cases findings from other countries might provide a better evidence base for policy action than pure assumptions about the reality. On the other hand, for countries with available data, comparative research can even enhance existing knowledge. If a certain empirical finding – e.g. the positive correlation between internet skills and the likelihood of having risky experiences – holds true in different cultural contexts, it can be regarded as a solid piece of knowledge that should be taken into account in the process of policy development.
Defining Policy Priorities

Studies following Kohn’s third option (“countries as a unit of analysis”) examine the relations among dimensions along which countries vary (see Figure 2). The first step of this kind of approach is to assess a certain indicator in all selected countries and to compare the results. Examples would be the average level of online skills or the percentage of children who have been bullied on the internet. In many cases comparative studies on media use stop at this point and present their results as a country ranking.

Figure 2. Logic of the “Countries as a Unit of Analysis / Benchmarking” Approach

Within the process of globalisation the logic of international benchmarking has become increasingly important. If a country has data indicating that a certain percentage of children or young people encounters harmful experiences, it is hard to decide whether this particular percentage is ‘high’ or ‘low’ and, accordingly, whether policy action is required or not. In recent years, comparative studies have become a core argument for defining policy priorities: comparative data are taken as benchmarks; if a particular country is below the international average regarding internet skills, policy makers will be highly motivated to develop initiatives to increase media literacy. In this case, comparative data do not directly enhance the knowledge base; instead they reflect the relative position of a country compared to other countries and therefore have a strong motivational impact on policy making.

Explaining Country Differences

In some cases the comparative approach, which defines countries as units of analysis, goes beyond mere benchmarking: this more ambitious kind of comparative research sets out to explain the differences between countries by investigating additional factors on the country level (see Figure 3). An example would be to ask whether the intensity of ICT regulation and the implementation of media literacy in the curricula of the educational system go along with a higher or lower likelihood for children to be bullied on the internet.
This approach is particularly useful for the development of policy initiatives. If there is empirical evidence that the low level of online skills in a particular country is linked more with specific patterns of parental mediation than with aspects of technical access, this finding may lead to the recommendation to invest more efforts in developing parents’ digital skills than in developing the technical infrastructure.

**Developing Transnational Activities**

The comparative options mentioned so far stay with a conception of the country or nation as a container; the respective research projects investigate commonalities and differences between countries. This is not necessarily the case in the final option distinguished by Kohn ("countries as part of a larger global system"; see Figure 4). The main objective of this kind of approach is to investigate transnational phenomena and how they can be observed in different countries. An example would be to investigate Facebook or YouTube users from all countries and how they make use of these communicative options.

This kind of evidence provides a knowledge base for transnational policy initiatives, for example with regard to the regulation of transnational online services like Facebook and other social networking sites (see Livingstone, Ólafsson and Staksrud 2011) or the implementation of transnational content classification systems (see Livingstone, Ólafsson, O’Neill, and Donoso 2012; Staksrud and Kirksaether, this volume).
The comparative work of the EU Kids Online network allows for the application of all the approaches mentioned above. In the next section we demonstrate selected results that reflect important differences between countries and discuss them with regard to their relevance for developing safer internet policies. In so doing, we focus mainly on the approach as presented in Figure 3. Thus, we start from relevant country differences regarding children’s online experiences and then try to identify country factors that explain these differences.

### Reviewing Empirical Evidence on Country Differences

Following the areas of interest of the EU Kids Online network, we present selected indicators for children’s online use, their online skills, the risks they encounter, and the harm they experience.

#### Online Practices

‘At what age should go online?’ is a question frequently asked by children’s organisations, NGOs and policy makers. Unfortunately, there is no “right” answer as going online younger has advantages and disadvantages. The more children use the internet, the more they gain digital literacy, and the more opportunities they take up, the more risks they also encounter (Livingstone and Helsper 2010). The EU Kids Online survey (Livingstone, Haddon, Görzig and Ólafsson 2011) showed how old children were across Europe when they started to use the internet. In general, the results show that the younger the children are, the earlier they went online for the first time. The youngest group claimed to go online at the age of seven, whilst older teenagers reported that they first went online at around the age of eleven. Are these differences also connected to country differences? The initial analysis of cross-country comparisons (Lobe, et al. 2011) shows that the youngest children to go online (age seven and eight) were in Nordic countries (Sweden, Denmark, Finland, Norway) and wealthier Western European countries (UK, Netherlands). Looking at the country level
factors, we can observe that these are the countries with the highest broadband penetration of 70-80%. Further, these countries are also the countries with the longest period (seven years) since 50% of households had access to the internet in Europe. Looking at the GDP per capita, the countries with the youngest children going online are also the wealthiest countries amongst those European countries studied (Lobe et al. 2011).

On the other side, children in Greece, Italy, Turkey, Cyprus, Germany, Austria and Portugal were amongst the oldest to first go online. Considering the country level factors, these countries can be divided into two groups. The first group includes Mediterranean countries with the lowest/lower broadband penetration in Europe, the shortest period since 50% of households accessed the internet and lower GDP per capita (Turkey, Greece, Portugal and Cyprus, Italy). The second group includes Germany and Austria, which are above the European average with regard to broadband penetration and the number of years since 50% of households went online; there was no variable in our data set that can plausibly explain why children in these two countries start using the internet at such a late age. An ad hoc explanation would conclude that these countries, in contrast to the Nordic countries, are rather sceptical towards new technology and concerned about their potential negative impact, thus they do not embrace the opportunities linked with the internet.

The average usage (time spent online) closely follows the above pattern with several exceptions. Bulgaria and Romania are countries with the highest internet use along with Scandinavian countries, and yet these two countries lag considerably behind in broadband penetration (less than 30%) and have the shortest period since 50% of households had access to the internet (less than one year). This might suggest that precisely this lag contributed to a greater excitement and promotion of internet use in these countries.

The EU Kids Online survey also examined seventeen different kinds of online activity practiced by children. Overall, of the full range of activities surveyed, children on average undertake nearly half of these (7.2 activities on average; see Lobe et al. 2011). On an individual level, the number of activities in which children engage increases with their age and years of internet use. On a country level, children in Lithuania and Cyprus report above-average diversity of online activities. Lithuania is amongst the countries with above average expected years of schooling whilst in Cyprus, the percentage of schools with classroom computers might be the country level factor that contributes to such a range of diverse online activities amongst children. The lowest range was reported by children in Ireland and Turkey. The Irish results are rather surprising as Ireland is the country with the longest expected years of schooling and has one of the highest levels of schools with computers in the classroom. However, the level of digital skills in Ireland is slightly below the European average. The general observation is that countries, in which
children report a lower level of digital skills, also display a smaller range of online activities (Lobe et al. 2011).

**Online Skills**

With regard to online skills, children on average report having four out of eight skills (Livingstone, Haddon, Görzig, and Ólafsson 2011). Teenagers claim considerably more skills than younger children. The differences in digital skills might not only occur between children, but also between European countries (see Lobe et al. 2011). The highest scores in online skills (average five and higher) are reached in the Nordic countries (Sweden, Norway, and Finland have the highest scores in Europe), in the Netherlands, and in some Eastern European countries (Slovenia, Estonia, Czech Republic). We examined whether these scores can be explained by differences between educational systems, taking into consideration the number of years of schooling that an adult in that country is expected to go through and the percentage of schools that offer and use computers in classrooms. It appears that the expected years of schooling and the percentage of schools with computers in classrooms are amongst the highest in Finland, Slovenia and Norway. In Sweden, the expected years of schooling is average but the percentage of schools with computers in classrooms is well above average.

The analysis suggests that digital and safety skills are higher in those countries with a better educational system. However, the Czech Republic and Estonia are exceptions to this conclusion; both the average or below average years of schooling and considerably lower share of schools with classroom computers and the high digital skills in these countries might be attributed to the individual differences amongst children.

The lowest level of self-reported skills was reported by Turkish children, which happens to be the country with the lowest broadband penetration and the shortest period since 50% of households had access to internet. Turkey is also the country with the lowest expected years of schooling in Europe (below 12). Overall, we might conclude that countries with more years of compulsory schooling are significantly more likely to have above-average digital skills. Similarly, children from the countries with the highest percentage of schools that offer and use computers in the classroom (above 45% of schools and more) are significantly more likely to have better digital skills (Lobe et al. 2011).

**Risk Experiences**

Overall, the highest percentage of risks experienced by children was in North East Europe – Estonia and Lithuania have the highest percentages, closely followed by Sweden and Norway, Finland and Denmark. Countries with the
lowest level of risk encountered online are Western and Southern European countries, the lowest percentage being in Turkey, Portugal, Greece and Italy (Lobe et al. 2011). On an individual level, high risk countries closely correspond with those that have children who report going online at an earlier age, to be heavier internet users, to score higher in digital and safety skills and who engage in a wider range of online activities. On a country level, children from countries with a higher broadband penetration are significantly more likely to have encountered more online risk. Countries with more online risk and high broadband penetration are the Nordic countries and Estonia. In Nordic countries in particular, initiatives to promote children’s rights and freedoms are widespread and this might explain the higher level of risk.

However, Eastern European countries, such as Bulgaria and Romania, encounter more online risk despite a lower broadband penetration. There also seem to be countries (Ireland, Spain, the UK and Germany) that indicate that despite the high broadband penetration, the risk can be low, possibly because of active efforts at risk reduction and safety awareness. This suggests that broadband access is a factor that contributes to more online risk, whether it be in ‘new risk’ countries such as Eastern Europe, or ‘high risk’ countries such as Nordic countries.

Further, the countries with a longer period (more than 3.7 years) since 50% of households had access to the internet are significantly more likely to experience more online risk. These countries are Slovenia, the Nordic countries and Estonia. Ireland and the UK are countries with more years of usage and a lower degree of risk. Likewise, countries with less than approximately three-and-a-half years since 50% of households had access to the internet are significantly more likely to experience less online risk. The only two countries with more recent usage and high risk are the Czech Republic and Lithuania. This might suggest that in the preponderance of countries where low risk is associated with only recent mass internet use, risk is set to rise, as in the well-established internet-using countries with high risk (Lobe et al. 2011).

Another country level factor that shapes the cultural context of risky experience is the press freedom index. In relation to our topic, this index can be interpreted as an indicator of a country’s general tendency to avoid direct regulatory instruments in the area of communication including safer internet issues. The analysis has shown that the countries with more press freedom, such as Nordic and Baltic countries, are also significantly more likely to have children who encounter a relatively high degree of online risk. In countries with more press freedom, there is possibly less internet regulation, and as a result potentially more online risk for children. However, as a counter example, Slovenia is a country with less press freedom and more online risk (Lobe et al. 2011).
Harmful Experiences

The EU Kids Online survey also measured harmful or upsetting aspects of children’s experience online (Livingstone, Haddon, Görzig, and Ólafsson 2011). Results have shown that a sizeable minority of children (one in eight) reported to be bothered by something on the internet in the year prior to survey. On an individual level, there are some differences by age between children. The youngest children are least likely to have been bothered by something online (9%) compared with older children (11-15%).

On a country level, the results show that more or less a quarter of children are bothered by something on the internet in Nordic-Baltic countries – Denmark (28%), Estonia (25%), Norway (23%), and Sweden (23%). Children in these countries have reported that they have experienced at least double the European average of reported harm (12%). Notably, less harmful experiences were reported by children in Italy (6%), Portugal (7%) and Germany (8%). Looking at individual level differences, countries with the highest percentage of children being bothered by something on the internet are countries with the highest percentage of children that start using internet for the first time at quite a young age (seven or eight years old), mainly use internet daily and for a considerable amount of time. On the contrary, the countries with the lowest percentage of children bothered by something online are the countries with the highest age of first use in Europe (age of ten), and average or below average percentage of daily users (Livingstone, Haddon, Görzig, and Ólafsson 2011; Lobe et al. 2011).

With regard to country level factors, the first apparent pattern shows that there is definitely a connection between harmful experiences and the number of years since 50% of households had access to internet: Nordic countries are the ones with the longest period (7 years) and Italy and Portugal are the countries with the shortest period since 50% of households had access to internet. The exceptions to this pattern are Estonia (which has an average period) and Germany, which is also amongst the countries with the longest period since 50% of households gained access to internet but is able to maintain a low percentage of children that have been bothered by something online. As for the risk experience, also for being bothered by something on the internet, press freedom might be one of the underlying factors to explain this.

The above examples show that country differences regarding children’s online practices and experiences partly correspond with country indicators. In their comprehensive report on country comparisons, Lobe et al. (2011) summarize the role of country indicators as follows (see also O’Neill, et al. 2011): there is a positive and significant effect of GDP per capita (as an indicator for the economic context) on the level of risk within a country. Countries with greater press freedom (as an indicator of the regulatory framework) are more likely to have higher levels of children’s use of the internet as well as higher
levels of online risk. Similarly, countries with higher broadband penetration are more likely to experience online risk, though there are exceptions. Children’s daily use of the internet is highest in those countries that have enjoyed internet access for longer, e.g. the UK and Nordic countries where penetration rates have exceeded 50% for at least 6 years. Educational factors such as expected years of schooling or the availability of computers in schools do not have an effect on levels of online usage or risk.

Types of Cultural Contexts: Classifying Countries

Developing policies for a large number of countries – e.g. the 28 members of the European Union or the 25 countries involved in the EU Kids Online II survey – requires some effort in reducing complexity. Although no country has exactly the same characteristics as any of the other countries, identifying groups of countries that are similar to each other is an important step towards a compromise between over-differentiation, i.e. taking single countries as unique cases, and over-simplification, i.e. taking the European average as an indicator for all countries. The empirical examples outlined above have shown that there seem to be intuitive clusters of countries with similar findings, e.g. “Northern” or “Mediterranean” countries.

Unfortunately, beyond this intuitive, mostly geographical clustering, there is no agreed classification of European countries in terms of cultural contexts; there is even no agreed selection of indicators along which cultural contexts can be assessed. And, as the examples above have shown, in most cases there are some exceptions that do not seem to fit into the overall pattern and that are hard to explain. Therefore the EU Kids Online network applied alternative approaches to country classifications that differ with respect to the concrete indicators that have been used.

‘Bottom-up’ Classifications

One approach to country classifications builds directly on the kind of empirical evidence as presented in the previous section, i.e. children’s behaviours and experiences. A simple case would be a classification based on a single indicator such as the number of internet skills (see Figure 5), by grouping the countries into ‘high skills’ (more than 5 skills), ‘medium skills’ (4-5), and ‘low skills’ (less than 4).

This kind of approach becomes more differentiated with any additional variable; an important pair of variables for the network has been the percentage of children per country who use the internet every day and the percentage who have encountered at least one online risk. One option to define country
clusters would be the four groups that result from taking the average of the two variables as a threshold between ‘high’ and ‘low’ countries.

Since these approaches are quite dependent on a few variables, a more ambitious approach is to classify countries on the basis of a number of theoretically
selected variables by means of cluster analysis or similar statistical procedures. Lobe et al. (2011: 39) have proposed the following classification, which is based on nine indicators for usage and different kinds of risks.

<table>
<thead>
<tr>
<th>Lower Risk</th>
<th>Higher Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT, BE, DE, FR, EL, HU, IT</td>
<td>CY, FI, NL, PL, SI, UK</td>
</tr>
</tbody>
</table>

Table 1. Country Classification of Online Use and Risk

This kind of classification can be regarded as a useful step towards nationally-specific policy recommendations. Children’s online practices and experiences in the four groups of countries clearly differ from each other; accordingly the EU Kids Online network has emphasized different priorities for policy initiatives. The general rule that follows from this classification is that high use of the internet is rarely if ever associated with low risk and high risk is never associated with low use. “This entails for policy makers the dilemma that promoting greater use and more online opportunities will inevitably increase the likelihood of greater exposure to risk” (O’Neill et al. 2011: 40) Given this general dilemma, policy initiatives in the four groups of countries have to start from different places and to emphasize different objectives. Just to cite two examples: while it is recommended that the ‘lower usage, lower risk’ group of countries should consider initiatives on how to further online skills and the range of online practices in order to make more use of the many opportunities provided by the internet, the ‘higher usage, higher risk’ group should focus on measures that can reduce the potential risk and harm linked with more intensive use of the internet.

‘Top Down’ Classifications

The ‘bottom-up’ approach as presented above easily leads to classifications of countries. However, these classifications are difficult to understand in terms of underlying country factors that can explain the respective differences or, indeed, the reasons why particular countries belong to any one group. In most cases we find ‘exceptions’ that are difficult to understand. Therefore, there are good reasons to also try a more systematic approach to country classifications that starts from a conceptual basis and sets out to operationalize the fuzzy concept of ‘cultural context’. At this stage, it is only possible to make an initial step in this direction.

So far, ‘cultural context’ has been used in the broad sense of the term in order to emphasise country differences in general. The model proposed in Figure 7
(see Hasebrink 2012) distinguishes four sub-dimensions of this broad concept: a) political/legal context, b) economic/technical context, c) societal context, and d) cultural context in the narrow sense of the term. The political and legal context together with the economic and technical context influence children’s online usage and experience primarily through the technical infrastructure and the concrete online services and contents, which are made available for children. The societal and the cultural context primarily shapes the everyday practices, the habits, and the particular opportunities of children. Children’s online usage and experiences can then be regarded as the outcome of the interaction between these two structuring patterns. This model is meant as a starting point for a more systematic ‘top-down’ approach to country classifications; future work of the EU Kids Online network will set out to elaborate on and to develop a meaningful classification.

**Figure 7.** Factors Influencing Children’s Online Practices, Skills, and Experiences

Conclusions and Outlook

In this chapter we have discussed the role of cultural context in the development of policy recommendations for internet safety. It is quite obvious – in a global perspective – that even within the homogeneous region of Europe, there are remarkable differences between countries in terms of children’s online practices and experiences: cultural context matters. As has been shown above, empirical evidence on commonalities and differences between countries can
inform policy decisions in several respects: it can enhance knowledge about factors that influence online skills on the one hand or online risk and harm on the other hand; it can widen the horizon of national policies by demonstrating ‘unknown’ practices and policies from other countries; it can help to define priorities for policy action by providing benchmarks; it can help to identify national factors that explain the respective children’s patterns of usage and experience; and it allows for the development of joint policies across countries.

The selected differences between countries provide some evidence on the kind of differences between children from different European countries and on country factors that go along with these differences. These factors can be regarded as indicators for specific cultural contexts that influence or shape children’s behaviours and experiences. With regard to policy implications this means that – beyond general consequences that seem to be relevant throughout Europe – specific recommendations have to be developed for European regions or even single countries (O’Neill, et al. 2011: 39).

Countries in which children become internet users at the youngest age (Nordic, Western European, some Baltic and Eastern European countries) should draw attention to younger children and find ways to promote safety skills and tools for raising awareness and supporting these young users as well as their parents, educators, caregivers, and schools. Data shows that children aged six to eight find themselves in a digital skills gap due to a lack of parental knowledge as well as a lack of digital literacy related topics in school syllabi for younger children. National campaigns and events should be initiated in order to address the parent-to-parent and within-family (as opposed to school-to-parent, and school-to-children) digital literacy and safety skills education, with the help of national awareness centres and similar institutions. Parents should be encouraged to talk to their children on a regular basis about their internet use as opposed to simply using filtering and blocking software. Training and advice should focus more than ever on providing simple safety and privacy messages and tools, using not solely text but also video and audio materials that are easier to use and understand by the ever-younger users. Further, emphasis should be placed on providing more high quality, age appropriate positive content online for younger groups of children in their national languages.

In countries with the highest number of self-reported digital and safety skills as well as the countries with the widest range of online activities, the educational system plays a significant role. In Nordic and Eastern European countries, where expected years of schooling are higher and the percentage of schools that offer computers in the classroom is higher, children have more skills. This might suggest that digital and safety skills are best learnt in schools which are also highly likely to have supporting awareness-raising material provided by national awareness centres in the form of brochures, competitions, and educative events. Therefore, countries with lower digital skills among children
should encourage schools to start updating their syllabi and to offer content that enhances digital skills and safety awareness.

Countries with the longest period since 50% of households have had access to the internet and high online risk encounters (Nordic and Western wealthier countries) should re-examine their awareness raising strategies. These countries have experienced and creative young users who use the internet as an integral part of their early lives. Children in these countries often engage in online activities that have not been designed for their age group. Therefore, initiatives for creating more positive and age-appropriate content opportunities are needed in such countries. At the same time, it is important to educate children in critical consumption of online content. Simple tools to distinguish between bad and good quality online quality should be designed and offered to children.

In order to go beyond the level of single countries, we discussed different approaches to country classification that can help to identify types of cultural contexts with similar experiences of children and, as a consequence, similar recommendations for policy initiatives. Starting from some ‘bottom-up’ classifications, we presented first considerations for a more systematic ‘top-down’ approach. While this approach will have to be elaborated as a part of future work of the EU Kids Online network, we conclude with three lessons learnt while dealing with the question of how cultural context influences children’s online practices and experiences and consider the consequences this may have for policy:

1. There are country differences with regard to children’s online practices and experiences; therefore there are different reasons for policy implications.
2. There are country differences in how certain patterns of online practices and experiences are evaluated; therefore there are different objectives for policy implications.
3. There are country differences with regard to the policy process or policy culture; therefore there are different styles of policy implications.

To be culture-sensitive, recommendations for safer internet policies have to consider all three dimensions of cultural differences.

Notes
2. Used the internet for schoolwork; played internet games on your own or against the computer; watched video clips; visited a social networking profile; used instant messaging; sent/received emails; read/watched the news on the internet; downloaded music or films; put or posted
photos, videos or music to share with others; played games with other people online; put or posted a message on a website; used a webcam; visited a chat room; used file-sharing sites; created a character, pet or avatar; spent time in a virtual world; written a blog or online diary.

3. Bookmark a website; block messages from someone you don’t want to hear from; find information on how to use the internet safely; change privacy settings on a social networking profile; compare different websites to decide if information is true; delete the record of which sites you have visited; block unwanted adverts or junk mail/spam; change filter preferences.

4. This reflects the degree of freedom of journalists and news organisations and the efforts made by the authorities to respect and ensure respect for this freedom. Source: http://en.rsf.org/IMG/pdf/classement_en.pdf

5. ‘Bothered’ was defined as: ‘for example, [something that] made you feel uncomfortable, upset, or feel that you shouldn’t have seen it’.

References


Chapter 16

Rights v. Restrictions

Recognising Children’s Participation in the Digital Age

Sharon McLaughlin

The child/media relationship is an entry point into the wide and multifaceted world of children and their rights – to education, freedom of expression, play, identity, health, dignity and self-respect, protection … in every aspect of child rights, in every element of the life of a child, the relationship between children and the media plays a role.¹

On 20th November 1989, the General Assembly of the United Nations (UN) adopted the United Nations Convention on the Rights of the Child (UNCRC, 1989). The UNCRC is the most universally accepted international convention, having been ratified by 193 countries (with the exception of the US, Somalia and South Sudan).² It enumerates civil, cultural, economic, political and social rights for children, defining a “child” as “every human being below the age of eighteen years.”³ In essence, the UNCRC is the international benchmark for children’s rights. The rights enshrined in the Convention are often classified into three distinct categories: rights of protection, provision and participation – the so-called ‘3Ps’.

The statement cited at the opening of this chapter was made on the 10th anniversary of the UNCRC at a meeting in Oslo organised by the Norwegian government and UNICEF and involving children, young people, media professionals and child rights experts. At this meeting, States parties to the UNCRC were challenged to take forward the media and communication aspects of the Convention (Livingstone 2009). A number of Articles of the Convention merit consideration in this context: Article 12 on the child’s right to be heard; Article 13 on the child’s right to freedom of expression; Article 14 on the child’s right to freedom of thought, conscience and religion; Article 15 on the child’s right to freedom of association and assembly; Article 16 on the child’s right to privacy; and Article 17 on the child’s right to freedom of information.⁴ The UNCRC has been ratified by all Member States of the European Union (EU) and the European Commission itself has recently affirmed that the “standards and principles of the UNCRC must continue to guide EU policies and actions that have
an impact on the rights of the child” (European Commission 2011). Thus, the
UNCRC constitutes an appropriate backdrop against which to frame European
law and policy impacting on children’s use of information and communication
technology (ICT) and, by extension, impacting upon children’s rights.

While notions of protection and provision are reflective of the more tradi-
tional view of children as dependent beings – reliant on others (namely, parents
and the state) to provide for and protect them – the concept of participation
embodies a novel approach to children and childhood, and one which is in-
creasingly advocated in relation to children’s relationship with ICT. It is for this
reason that this chapter will focus on children’s participatory rights. Specifically,
by examining in detail Article 12 (right to be heard), Article 13 (right to freedom
of expression) and Article 17 (right to information), this chapter will illustrate
the centrality of the concept of participation when it comes to the creation of
an internet that is truly better for children.

According to the UN Committee on the Rights of the Child (hereinafter
referred to as the Child Committee), the body of independent experts respon-
sible for monitoring implementation of the UNCRC by States parties⁵, the term
participation is:

[…] widely used to describe ongoing processes, which include information-
sharing and dialogue between children and adults based on mutual respect,
and in which children can learn how their views and those of adults are taken
into account and shape the outcome of such processes.⁶

The active and meaningful participation of children in society is a pivotal
component of all aspects of child development – cultural, mental, moral and
social. In this digitised landscape, child participation in the ICT environment
undoubtedly constitutes an important, even fundamental, aspect of child de-
velopment and maturation.

Article 12 UNCRC: The Right to be Heard

Article 12 UNCRC provides:

1. States parties shall assure to the child who is capable of forming his or her
own views the right to express those views freely in all matters affecting the
child, the views of the child being given due weight in accordance with the
age and maturity of the child.

2. For this purpose, the child shall in particular be provided the opportunity
to be heard in any judicial and administrative proceedings affecting the child,
either directly, or through a representative or an appropriate body, in a man-
ner consistent with the procedural rules of national law.
Article 12 ascribes to children the right to be heard in all matters affecting them, to participate in all decision-making processes having a bearing on their lives and to exert influence over such decisions in accordance with their age and maturity. It places an obligation on States parties to involve children in all matters affecting them – not to compel children to express their views nor pressurise them into becoming delegated decision-makers (Van Bueren 1998). The right of the child to be heard is not analogous to a right to be listened to; rather listening to the views of children is but one link in the chain of participation (Child Committee 2006; Archard 2004). The creation of a better internet for children is undoubtedly a matter ‘affecting the child’ – thus, it follows that children should be actively and meaningfully involved in the various debates and challenges surrounding this matter. Moreover, the fact that policies and actions directed at the creation of a better internet for children (at least sometimes) involve placing restrictions, even prohibitions, on children’s use of ICT, makes it difficult to claim that such measures do not fall within the general scope of ‘matters affecting the child’.

According to the Child Committee (2009), Article 12 “manifests that the child holds rights which have an influence on her or his life, and not only rights derived from her or his vulnerability (protection) or dependency on adults (provision).” In relation to the interpretation of the phrase ‘capable of forming his or her own views’, the Child Committee (2009) has stated that:

[…] it is not necessary that the child has comprehensive knowledge of all aspects of the matter affecting her or him, but that she or he has sufficient understanding to be capable of appropriately forming her or his own views on the matter.7

This interpretation is particularly important in the context of the internet; an environment in which children may possess the technical skills and abilities to use ICT but may not understand the infrastructure behind the technology or the full implications of use. According to the Child Committee (2009), “sufficient knowledge” is all that is required when it comes to children’s exercise of their right to be heard. It is argued that Article 12 is particularly significant in circumstances where children may be possessed of “superior knowledge” to that of adults (Van Bueren 1998). Considering that children are often portrayed (rightly or wrongly) as being more technologically astute than adults, this contention has particular resonance in the context of the online environment.8 Article 12 is considered “an integral part of the implementation of the other articles of the Convention” (Child Committee 2006) and applies to all children capable of forming views and not merely those capable of expressing views (Van Bueren 1998). The inclusion of two criteria – age and maturity – was a deliberate move by the drafters of the Convention to ensure that States parties “should not have an unfettered discretion as to when to consider and when to ignore the views of a child” (Van Bueren 1998).
In 2009, the Child Committee issued a General Comment on the right of the child to be heard in which it reaffirmed the right to be heard as one of the four general principles of the Convention. The right to be heard, it stated, is closely correlated to the right to freedom of expression (Article 13) and the right to information (Article 17), both of which are considered later in this chapter.

Article 13, on the right to freedom of expression, and article 17, on access to information, are crucial prerequisites for the effective exercise of the right to be heard. These articles establish that children are subjects of rights and, together with article 12, they assert that the child is entitled to exercise those rights on his or her own behalf, in accordance with her or his evolving capacities.

According to the Child Committee (2009), “[t]he views expressed by children may add relevant perspectives and experience and should be considered in decision-making, policymaking and preparation of laws and/or measures as well as their evaluation.” This statement is especially applicable to the online environment where, as mentioned, children are often represented as being particularly savvy. Children should therefore be meaningfully involved in the debates and decision-making processes leading to the formulation of law and policy directed at the creation of a better internet for children. The Child Committee (2009) further stated that “[t]he concept of participation emphasizes that including children should not only be a momentary act, but the starting point for an intense exchange between children and adults on the development of policies, programmes and measures in all relevant contexts of children’s lives.” The online environment inarguably constitutes one such ‘relevant context’.

According to the Child Committee, the phrase “administrative proceedings”, contained in Article 12(2), includes “decisions about children’s education, health, environment, living conditions, or protection.” Debates and challenges surrounding the creation of a better internet for children are capable of falling within several of these headings. The Child Committee’s General Comment also refers to the important role played by the media in “promoting awareness of the right of children to express their views, and of providing opportunities for the public expression of such views”, encouraging “various forms of the media to dedicate further resources to the inclusion of children in the development of programmes and the creation of opportunities for children to develop and lead media initiatives on their rights.”

The Child Committee further asserts that the right of the child to be heard within the educational setting is integral to the realisation of the right to education, enshrined in Articles 28 and 29 UNCRC. The importance of education when it comes to the creation of a better internet for children – in particular, the creation of a safer internet for children – is frequently referred to in policy circles, and it is widely accepted that education is a crucial component of any response to fostering greater safety online. If one accepts the Child Committee’s
assertion that the right of the child to be heard is central to the realisation of the right to education, then it follows that those with responsibility for educating children – and not only teachers in the formal educational setting – have an important role to play in increasing children’s awareness and understanding of Article 12, and in creating an environment conducive to the exercise of the right contained therein. The formal educational setting, in particular, offers (at least potentially) an appropriate and fecund forum in which children can make themselves heard on various issues, including issues related to online risk and opportunity. According to the findings of EU Kids Online, 63% of European 9-16 year olds use the internet at school or college, making it the second most common location, after the home (87%), for going online (Livingstone et al., 2011). This finding means that schools, and the wider educational community, are uniquely placed to engage with children on matters related to the creation of a better internet, and to ensure the views of children on such matters are heard.

The Child Committee, in its General Comment, welcoming the expansion of the concepts of peer education and peer counselling, attributes particular importance to children’s expression of their views in matters relating to the “elimination of discrimination, prevention of bullying and disciplinary measures.” This assertion lends further credence to the position that children’s views on online risks, such as cyberbullying, should not only be heard but also afforded due consideration. Class councils, student councils, student representatives on boards and committees are all considered effective means of achieving child participation and of providing children with the opportunity to be heard when it comes to the formulation, implementation and enforcement of their school’s policies and codes of behaviour. EU Kids Online found that 44% of European 9-16 year olds had received internet safety advice from their peers and that, if something online had upset them, children overwhelmingly confided in a friend (Livingstone et al. 2011). According to Livingstone et al. (2011), peer mentoring schemes, the benefits of which are “easily neglected”, have a valuable role to play if “constructively harnessed” (Livingstone, et al. 2011). Such schemes and initiatives, if adequately recognised and resourced, would go some way towards facilitating children’s participation, as stakeholders, in discussions surrounding the creation of a better internet.

The Child Committee, also in its General Comment on the right to be heard, notes that “[c]hildren require play, recreation, physical and cultural activities for their development and socialization” and that these activities “should be designed taking into account children’s preferences and capacities.” There is no disputing that the internet and associated technologies are important recreational and cultural tools for the vast majority of children today. The Child Committee further asserts that “[c]hildren who are able to express their views should be consulted regarding the accessibility and appropriateness of play and recreation facilities.” This remark is particularly applicable to children’s
participation in the online environment wherein children’s access to technology is often restricted on grounds of the inappropriateness of certain activities and materials. The Child Committee proposes that signatories to the UNCRC “avoid tokenistic approaches, which limit children’s expression of views, or which allow children to be heard, but fail to give their views due weight.” In summation, the General Comment on the Right of the Child to be Heard states that:

Investment in the realization of the child’s right to be heard in all matters of concern to her or him and for her or his views to be given due consideration, is a clear and immediate legal obligation of States parties under the Convention. It is the right of every child without discrimination.

Article 13 UNCRC: The Right to Freedom of Expression

Article 13 UNCRC provides:

1. The child shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child’s choice.

2. The exercise of this right may be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
   (a) For respect of the rights or reputations of others; or
   (b) For the protection of national security or of public order (ordre public), or of public health or morals.

At the outset, it is worth noting that the original draft Convention, submitted by Poland to the UN Human Rights Commission on 7th February 1978, did not contain any reference to the child’s right to freedom of expression (Van Bueren 1998). Article 13 ascribes to the child the right to “seek, receive and impart information and ideas of all kinds” through any medium. The right to “seek” information, it is suggested, implies the carrying out of some form of investigative action (Van Bueren 1998). For example, it is likely that conducting a search using a search engine would amount to an exercise of one’s right to seek information. The right to “receive” information, therefore, might reasonably be interpreted as a right to consume the information retrieved as a result of this investigative process. The child’s right to impart information to others is of particular importance in the context of the online environment as children are no longer mere receptacles (or consumers) of content but are also creators and distributors of such content. As noted above, the right to freedom of expression contained in Article 13 is closely related to the right to be heard (Article 12) and the right of access to information (Article 17).
The actual wording of Article 13 UNCRC is largely similar to that of Article 19 of the International Covenant on Civil and Political Rights (ICCPR) (Detrick, 1999). In fact, so similar is the wording that it has been contended that “there is little value in Article 13 itself as most parties to the UNCRC are parties also to the ICCPR and the travaux preparatoires show that Article 13 was simply ‘lifted’ from Article 19 ICCPR with little attempt to apply it to children” (Langlaude 2010). However, it is also asserted that the right to freedom of expression under Article 13 is more limited than that contained in Article 19 ICCPR (Lopatka 1996). Specifically, in addition to the restrictions contained in the second part of Article 13, the child’s exercise of the right to freedom of expression is limited by Article 5 UNCRC (Lopatka 1996). Article 5 requires States parties to “respect the responsibilities, rights and duties of parents” (and, where appropriate, those of the wider family and community) to direct and guide children in the exercise of the rights contained in the Convention “in a manner consistent with the evolving capacities of the child.” It is suggested that this additional limitation “is based on the fact that a child, by reason of his/her physical and mental immaturity, needs special safeguards and care” (Lopatka 1996). However, where parents or others with legal responsibility for children fail to provide appropriate direction and guidance, or abuse their rights as parents/guardians to curtail their child’s freedom of expression, it is asserted that the state has an obligation to intervene “for the good of the child” (Lopatka 1996). In addition to being interpreted in conjunction with Article 5, the child’s right to freedom of expression is also to be construed in line with Article 3 of the Convention, which embodies the ‘best interests’ principle. The notion that children’s ‘best interests’ should be placed at the centre of decision-making processes is in itself unproblematic. However, it is important to remain mindful of the main criticism of the ‘best interests’ principle – it is a “vague provision which gives enormous discretion to the decision-maker to impose his/her own judgment as to what the child’s welfare demands in a particular case” (Kilkelly 2010). Those involved in the formulation and implementation of law and policy directed at the creation of a better internet for children must remain cognisant of this criticism and do their utmost to ensure the concept of ‘best interests’ is not interpreted in a purely protectionist manner.

Article 13 UNCRC, unlike Article 19 ICCPR, does not make reference to the right to “hold opinions without interference” or to the “special duties and responsibilities” implicit in the exercise of the right to freedom of expression (Detrick 1999). In the absence of any specific explanation for the omission of the right to hold opinions without interference, it has been suggested that the drafters of the UNCRC may have considered this right already encompassed in Article 12 and/or Article 14, concerning the child’s right to be heard (discussed above) and the child’s right to freedom of thought, respectively (Detrick 1999). While this omission is not particularly detrimental to the right to freedom of
expression contained in Article 13, it has been maintained that it is somewhat illogical considering that the “mere holding of an opinion […] is a purely internal and personal ability uncontrollable by the state” (Van Bueren 1998). The reference to “special duties and responsibilities” contained in Article 19 ICCPR was considered necessary by drafters because of the “powerful influence the modern media of expression exerted upon the minds of men and upon national and international affairs” (Detrick 1999; Bossyut 1987). The right to freedom of expression was considered to be “a precious heritage as well as a dangerous instrument” and, as a result, the drafters of the ICCPR felt that the “duties and responsibilities in the exercise of the right should be especially emphasized” (Detrick 1999; Bossyut 1987). The inclusion of a similar reference in Article 13 UNCRC was “apparently not found necessary with regard to the child’s exercise of the freedom of expression” (Detrick 1999; Bossyut 1987).

It is possible that the drafters of the Convention believed that children – especially younger children – did not possess sufficient capacity to understand the concomitant duties and responsibilities attaching to the right to freedom of expression. However, despite the non-inclusion of the phrase “special duties and responsibilities” in Article 13, it is important that children of all ages are made cognisant of the fact that the right to freedom of expression carries certain duties and responsibilities. This is especially important in the context of the online environment in which children operate as both consumers and creators of expression and, in light of this dual role, must be made aware of the potential impact of their expressive activities. For example, according to findings from EU Kids Online, 12% of European 9-16 year olds report that they have acted in a nasty or hurtful way towards others (Livingstone, et al., 2011). Thus, while children should be encouraged to exercise their right to freedom of expression in the online environment, they should also be encouraged to exercise this right in a responsible and respectful manner.

At the time of the drafting of the UNCRC, the US delegation proposed the formulation of a single provision dealing with the child’s right to privacy, freedom of association and assembly and freedom of expression (Detrick 1999). According to the US, the inclusion of such a provision was necessary due to the fact that adolescents, encompassed in the definition of “child” contained in the Convention, are often possessed of the proficiencies necessary to participate fully and effectively within society and, as a result, must be ascribed civil and political rights and freedoms (Detrick 1999). Subsequently, the US contingent suggested the insertion of three separate provisions dealing with these rights, further contending that the ascription of such rights to children was necessary in order to shield children from potential abuses by government (Detrick 1999). As noted above, the US is currently one of only three countries that has not ratified the UNCRC.

It has been argued that the value assigned by society to the expressive con-
tributions of children, as well as the lack of avenues available to assist children in the articulation of their right to freedom of expression, could conceivably be regarded as “indirect restrictions” on their right to freedom of expression (Van Bueren 1998). In other words, a society’s failure to attribute due weight and consideration to the expressions of children, as well as to provide children with appropriate channels through which to enunciate such expressions, effectively impedes children’s exercise of their right to freedom of expression. As already noted, in light of the fact that the promotion of a better internet – more especially, the promotion of a safer internet for children – sometimes involves state-imposed restrictions (even prohibitions) on children’s access to certain types of expression (for example, sexual and violent expression), it is crucial that children are afforded real opportunities to make expressive contributions when it comes to the formulation of law and policy in this area. Moreover, it is important that the state actively encourage children to make expressive contributions in this regard.

Also at the time of the drafting of the UNCRC, the German Democratic Republic proposed the insertion of the phrase “or the spiritual and moral well-being of the child” into paragraph 2(b) of Article 13, to cover certain perils posed by the expression of violent information by the mass media (Detrick 1999). However, it was felt that the inclusion of such a phrase would place added restrictions on the right itself and, further, that concerns in relation to the dissemination of violent information were already addressed by Article 17, concerning the important function performed by the mass media (discussed below) (Detrick 1999). According to Van Bueren (1998), the concept of moral protection is “so subjective that in order to help prevent abuses, children ought to be entitled to exercise their right to freedom of expression and participate in determining whether it is in their best interests not to receive particular classes of information.” Meaningful participation in the assessment of whether or not certain types of speech are contrary to their best interests will necessitate educating children, from an early age, about the right to freedom of expression and all it entails. However, considering that such education will be delivered by adults (the state, in the form of the educational system, and parents), and taking cognisance of adults’ traditional reluctance to relinquish control when it comes to children’s participatory rights, perhaps there is a need for some level of input from children’s rights organisations when it comes to the delivery of education relating to children’s civil and political rights.16

According to Langlaude (2010), Article 13 “has been poorly interpreted by the Child Committee and adds little to the meaning of the child’s right to freedom of expression” (Langlaude 2010). However, the fact that the Child Committee often considers Article 13 alongside Article 17 (the right to information and the role of the media, discussed below) arguably sheds some light on its interpretation (Langlaude 2010). Despite frequently discussing the right
to freedom of expression in conjunction with other rights and freedoms, the Child Committee rarely elaborates on “how and why” such rights relate to one another (Langlaude 2010). Langlaude (2010) further maintains that the Child Committee’s “apparently holistic view of freedom of expression does not shed more light on the extent of the right itself.” In other words, despite being appended to, and regarded as important to the exercise of several other rights and freedoms, the actual scope of the child’s right to freedom of expression is seldom explicated. However, the Child Committee’s (2009) General Comment on the right of the child to be heard, stating that the right to be heard is closely correlated with the right to freedom of expression in Article 13 and the right to information in Article 17, proceeds to explain, at least to some extent, the way in which these rights are interconnected. Distinguishing between the right to freedom of expression and the right of the child to be heard, the Child Committee (2009) states that:

Freedom of expression relates to the right to hold and express opinions, and to seek and receive information through any media. It asserts the right of the child not to be restricted by the State party in the opinions she or he holds or expresses. As such, the obligation it imposes on States parties is to refrain from interference in the expression of those views, or in access to information, while protecting the right of access to means of communications and public dialogue.

Langlaude (2010) criticises the Child Committee for failing to provide a “consistent analysis” of Article 13, asserting that the provision of such analysis “does not seem to be a priority for the Child Committee which has, generally, neglected civil rights and freedoms.” In other words, it is the responsibility of the Child Committee to assist States parties in interpreting the scope and extent of the child’s right to freedom of expression under Article 13 through the provision of a “consistent analysis” of the right. Langlaude (2010) further refers to Article 13 as “the missing provision of the Convention”, stating that the failure of the Child Committee to provide a “clear theoretical underpinning of why the child has a right to freedom of expression and how the right applies to children of all ages but in different ways” is “regrettable.” Moreover, the Child Committee are accused of having failed to avail of the opportunity to “develop a sophisticated analysis of children’s civil and political rights” (Langlaude 2010). The need for this “sophisticated analysis” is even greater in light of the fact that children are now living in an information society; an environment in which they have access to a diverse range of content through a wide range of media platforms and in which they are active creators and disseminators of expression as well mere consumers of expression.
Article 17 UNCRC: The Right to Information and the Role of the Media

Article 17 UNCRC provides:

States parties recognize the important function performed by the mass media and shall ensure that the child has access to information and material from a diversity of national and international sources, especially those aimed at the promotion of his or her social, spiritual and moral well-being and physical and mental health.

To this end, States parties shall:

(a) Encourage the mass media to disseminate information and material of social and cultural benefit to the child and in accordance with the spirit of article 29;
(b) Encourage international co-operation in the production, exchange and dissemination of such information and material from a diversity of cultural, national and international sources;
(c) Encourage the production and dissemination of children’s books;
(d) Encourage the mass media to have particular regard to the linguistic needs of the child who belongs to a minority group or who is indigenous;
(e) Encourage the development of appropriate guidelines for the protection of the child from information and material injurious to his or her well-being, bearing in mind the provisions of articles 13 and 18.

Article 17 recognises “the important function performed by the mass media” and encourages States parties to “ensure that the child has access to information and material from a diversity of national and international sources.” States parties are also requested to encourage the mass media to broadcast information and material of social and cultural benefit to children. Further, States parties are encouraged to embolden the mass media to formulate guidelines to shield children from “information and material injurious to their well-being”, bearing in mind both the child’s right to freedom of expression and the responsibilities of parents in relation to the upbringing of their children. The right to information enshrined in Article 17 is closely correlated to both the right to be heard and the right to freedom of expression, discussed supra (Child Committee 2009).

The right to information embodied in Article 17 is particularly important in the context of the online environment. The internet is an information gateway; offering users access to a wealth of information on an infinite number of topics. The challenge, therefore, is to establish an equilibrium between children’s right to access information, on the one hand, and the legitimate interest in safeguarding children from accessing potentially harmful material, on the other. In respect of Article 17, the Child Committee (2009) has stated that:
Children need access to information in formats appropriate to their age and capacities on all issues of concern to them. This applies to information, for example, relating to their rights, any proceedings affecting them, national legislation, regulations and policies, local services, and appeals and complaints procedures. Consistent with articles 17 and 42, States parties should include children’s rights in the school curricula.

In other words, children are entitled to age-appropriate information on all proceedings, legislation, regulations and policies affecting their rights. When it comes to constructing law and policy directed at the creation of a better internet for children – an objective which clearly impacts on the rights of children – States parties should furnish children with age-appropriate information explicating both the need for, and objective of, such measures. Arguably, in terms of shielding children from potentially deleterious material, the wording of Article 17(e) – specifically, its reference to “appropriate guidelines” – intimates that the UN favours the implementation of codes and standards (that is, guidance-based measures) as opposed to laws and regulations in the more conventional sense. Article 17(e) neither explicates the meaning nor contains any examples of “information and material” considered injurious to children’s well-being. Article 17(e) places a positive duty on States parties to shield children from inappropriate material and, as such, “works so as to impose an additional restriction on the child’s right” to freedom of expression (Langlaude 2010). The UN General Assembly’s Resolution on ‘A World Fit for Children’ makes reference to the importance of “mass media information campaigns” in the prevention and discouragement of alcohol, tobacco and drug use, as well as to the role of the mass media in campaigns against sexual exploitation and trafficking of children (UN General Assembly 2002). The General Assembly (2002) clearly posits the view that the mass media have a pivotal role to play in terms of educating and informing the general public about risk issues:

The mass media and their organizations have a key role to play in raising awareness about the situation of children and the challenges facing them. They should also play a more active role in informing children, parents, families and the general public about initiatives that protect and promote the rights of children, and should also contribute to educational programmes for children. In this regard, the media should be attentive to their influence on children.

According to Langlaude (2010), while the Child Committee does refer to the need to strike a balance between access to information, on the one hand, and the protection of children from material injurious to their well-being, on the other, it places greater emphasis on protection than on access. It is further contended that the right of access to information contained in Article 17 differs from similar rights contained in other international law instruments in that it
imposes a positive obligation on States parties to provide access to information and materials from a diversity of national and international sources as opposed to a negative obligation not to “interfere with the right to access information that is generally accessible” (Langlaude 2010). Detrick (1999) observes that provisions equivalent to Article 17 “cannot be found in the major universal and regional general conventions on human rights.”

Article 17 originally referred to the media in somewhat negative terms, providing that States parties to the UNCRC should endeavour to “protect the child against any harmful influence that the mass media, and in particular the radio, film, television, printed materials and exhibitions, on account of their content, may extend on his mental and moral development” (Detrick 1999). This proposed phrasing caused considerable contestation among the delegations. On the one hand, some emphasised the importance of freedom of information and called for a more positively drafted reference to the mass media (Detrick 1999). On the other hand, it was argued that the protection of children from harmful media influences was deserved of particular attention and should not be viewed as a diminution of the significance of the right to freedom of information (Detrick 1999). The final phrasing of Article 17 attempted to reconcile these two opposing viewpoints. Detrick (1999) questions the fortitude of the obligations on States parties set out in Article 17, stating that the repeated use of the term ‘encourage’ makes the obligations contained therein “appear […] rather weak in nature.” In October 1996, the Child Committee held a Day of General Discussion on children and the media (Child Committee 1996). The Child Committee focused on three principal areas: the possibility for active participation by children in the media; the protection of children from harmful media influences through the media; and the improvement of the image of the child through media reporting. According to the Child Committee, it is in the spirit of Articles 12, 13 and 14 UNCRC – the right to be heard, the right to freedom of expression and the right to freedom of thought, conscience and religion, respectively – “that all children should not only be able to consume information material but also to participate themselves in the media.” The subsequent discussion, which included input from UN bodies, media representatives, academic institutions and – perhaps, most significantly – from children, resulted in twelve recommendations. With regard to the protection of children from harmful media influences, the Child Committee recommended the collation of information on voluntary agreements, mechanisms and standards between States parties and media industries. Furthermore, it recommended the compilation of a report on positive practical experiences of child participation in the media, as well as the promotion of child Internet forums, dedicated child libraries and media education.
Conclusion

The European Union’s (EU) approach towards children’s rights protection has evolved throughout the years, influenced by the pace of European integration, the development of the concept of European citizenship, demographic change and the EU enlargement. Until the 1990s, the issue of children’s rights was less relevant for the EU agenda and the EU had a rather limited competence in the field of fundamental rights. For the past decade, children’s rights have gradually taken on increased importance thanks to new competences acquired by the EU in this field. (European Parliament Citizens’ Rights and Constitutional Affairs Committee 2012)

Up until the entry into force of the Treaty of Lisbon in December 2009, the EU did not have a legal obligation to consider the effects of its actions on children, nor to ensure its policies were compatible with international children’s rights standards (that is, compatible with the UNCRC) (Children’s Charities Briefing, 2009). The Treaty of Lisbon added the promotion and protection of the rights of the child to the list of stated objectives of the EU (new Article 2 of the Treaty on European Union). The inclusion of the objective of protecting children’s rights provides a solid legal grounding upon which to develop and implement measures which will ensure that the EU, in all its policy areas (including audiovisual and media policy), affords due consideration to the rights of the child. The European Commission has committed to working for the protection, promotion and fulfilment of children’s rights in all internal and external EU actions and policies having an impact on children. The Commission’s Communication on ‘An EU Agenda for the Rights of the Child’, issued in February 2011, encapsulates this commitment (European Commission 2011). The Agenda contains eleven concrete actions to be taken by the Commission over the coming years, all of which aim to promote and protect the rights of children and improve the well-being of children in various aspects of their lives. In relation to the online environment, the Commission states that it will support EU countries and other stakeholders in strengthening the “participation of children” so that they can “make the most of online technologies” and counter online risks such as cyber-bullying and exposure to harmful content (European Commission 2011). The Commission, then, clearly recognises the protective function of participation – empower children’s participation in the online environment and, in so doing, empower children to manage online risks and enjoy online opportunities.

In addition to adding the protection of the rights of the child to the EU’s stated objectives, the Treaty of Lisbon made the EU Charter of Fundamental Rights (2000) legally binding on EU Member States. Article 24 of the Charter deals with the rights of the child and, in addition to stating that children “have the right to such protection and care as is necessary for their well-being”, also
stipulates that children “may express their views freely” and that these views “shall be taken into consideration on matters which concern them in accordance with their age and maturity.” Article 24, then, embodies the concepts of protection and participation – the right to “such protection and care as is necessary”, on the one hand, and reference to the right to freedom of expression and the right to be heard, on the other.

As already noted, notions of provision and protection sit comfortably with (adult) perceptions of children as vulnerable beings requiring the state and others (parents, educators, etc.) to provide for and protect them. The notion of participation, on the other hand, does not always sit comfortably with this particular conceptualisation of children and childhood. It is therefore important that the protective function of participation is emphasised – the idea that children must be permitted to participate in the online environment in order that they may become safe and responsible users of ICT. In other words, it is only through the process of participation that children learn to understand and manage the risks associated with the internet and to develop resilience.17 This is not to say that children do not require protection; but rather that participation must be recognised as a fundamental component of such protection. Going forward, it is important that all stakeholders afford due consideration to the nature and extent of the ways in which various preconceptions (and misconceptions!) of children and childhood shape policy and practice and, in so doing, must ensure their actions are based on evidence as opposed to assumption. In addition, children – as the subjects of such policies and practices – should be actively and meaningfully involved in decision-making processes (in so far as is possible).

Children are no longer mere consumers of content but are also creators of content (O’Neill and McLaughlin 2010). Approaches to teaching children to become safe and responsible users of online technologies must take account of the child’s dual role as consumer and creator. This dual role necessitates that actions directed at the creation of a better internet for children be framed against the backdrop of human rights. The UNCRC, as already noted, embodies rights of provision, protection and participation. This chapter focused on the right to be heard (Article 12), the right to freedom of expression (Article 13) and the right of access to information and the role of the media (Article 17). While these rights are interconnected, each – on its own merits – is fundamentally applicable to children’s relationship with the internet. Stakeholders in the policymaking process must strive to achieve an acceptable balance between shielding children from risk of harm, on the one hand, and ensuring children’s access to and use of the internet and new media technologies is not unjustifiably or arbitrarily impeded, on the other. The challenge, therefore, lies in establishing some form of equilibrium between protection and participation.

On 19 December 2011, the UN General Assembly approved a third optional protocol on a Communications Procedure, which will allow individual

315
children to submit complaints to the Child Committee regarding specific violations of their rights under the Convention and its first two optional protocols (United Nations 2011). This optional protocol to the UNCRC to provide a communications (or complaints) mechanism represents a huge step forward in the promotion and protection of children’s rights. The absence of such a mechanism was undoubtedly a manifest flaw of the Convention. After all, other UN human rights instruments such as the International Covenant on Civil and Political Rights (ICCPR), the Convention on the Elimination of Discrimination Against Women (CEDAW) and the Convention on the Rights of Persons with Disabilities (CRPD) have in place optional protocols allowing the responsible Committees (under certain circumstances) to consider individual complaints. At the time of the drafting of the UNCRC, the need to allow children to bring individual complaints before the Child Committee was considered but subsequently rejected both by countries and by the vast majority of non-governmental organisations (NGOs) on the basis that “such a procedure would inject contention into a treaty which had been negotiated by consensus” and “could possibly harm development work in developing states” (Van Bueren 2009). However, more than twenty years after the introduction of the Convention, and now that it has been ratified by such a large number of countries throughout the world, any such reservation must surely belong in the realms of history. It is crucial that children and their representatives are made aware of the complaints mechanism. To this end, the Child Committee must work closely with States parties in order to ensure that information on the complaints mechanism is disseminated as widely as possible and, more importantly, that it reaches those whom it is intended to benefit – children and child representatives. In addition, the Child Committee may, as a result of a complaint, be forced to elaborate on the nature, extent and application of certain rights guaranteed by the UNCRC. Providing children with an avenue through which to channel allegations of human rights violations is indeed a positive step forward. Nonetheless, the importance of human rights education cannot be overemphasised – it seems somewhat inane to speak of children’s rights (and indeed to speak of human rights generally) where the holders of such rights may be unaware or ill-informed of their entitlements.

Notes
3. Article 1 UNCRC provides: “For the purposes of the present Convention, a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier.”
4. There are, of course, other rights contained in the UNCRC which are relevant to children's relationship with ICT but discussion of which are beyond the scope of this chapter. For example, Article 34 on the child's right to protection from all forms of sexual exploitation and abuse; Articles 28 and 29 on the child's right to an education; and Article 31 on the child's right to play and recreation and to participate fully in cultural and artistic life.

5. Article 4 UNCRC requires State Parties to "undertake all appropriate legislative, administrative, and other measures for the implementation of the rights recognized in the present Convention." In addition, Article 44 places an obligation on States parties to undertake and submit periodic reports to the Committee on the Rights of the Child ("Child Committee"). Specifically, States parties are required to provide the Child Committee with information "on the measures they have adopted which give effect to the rights" enshrined in the Convention and "on the progress made on the enjoyment of those rights." States parties are obliged to submit the first such report within two years of ratifying the Convention, and every five years thereafter.


7. Ibid.

8. See further Chapter 5.

9. Along with the right to non-discrimination (Article 2); the best interests of the child as a primary consideration (Article 3); and the right to life and development (Article 6).


11. See further Chapter 5.

12. Article 31 UNCRC provides: 1. States Parties recognize the right of the child to rest and leisure, to engage in play and recreational activities appropriate to the age of the child and to participate freely in cultural life and the arts. 2. States Parties shall respect and promote the right of the child to participate fully in cultural and artistic life and shall encourage the provision of appropriate and equal opportunities for cultural, artistic, recreational and leisure activity. See also United Nations Committee on the Rights of the Child, General Comment No.17 (2013): The right of the child to rest, leisure, play, recreational activities, cultural life and the arts (Sixty-second session, Geneva, 14 January-1 February 2013).


14. See further United Nations Committee on the Rights of the Child General Comment No.14(2013) on the right of the child to have his or her best interests taken as a primary consideration (Sixty-second session, Geneva, 14 January-1 February 2013).

15. The other two countries are Somalia and South Sudan, the latter of which only recently (2011) became a Member State of the UN.

16. See further Chapter 10, this volume.

17. See, for example, d’Haenens et al., How to cope and build online resilience (EU Kids Online, 2013)

18. The protocol was opened for signature on 28th February 2012 and will enter into force once it has been ratified, or acceded to, by 10 signatory countries. See further United Nations Treaty Series, Status of Treaties: Optional Protocol to the Convention on the Rights of the Child on a communications procedure. As of 29th September 2013, eight signatory countries have ratified/acceded to the optional protocol.

References


Index

Acceptable Use Policy (AUP) 199
Accountability 16, 82, 85, 111-112, 189
Action Lines 26, 231, 233, 236, 242
Adolescents 63, 65-66, 70-72, 74, 261-262, 267, 308
Adult Chamber of Commerce 29
Adult Entertainment Broadcast Network 29
Age rating 13, 88, 113-117, 142
Algorithms 25, 33
America Online 29, 128
Application Programming Interfaces (APIs) 119-120, 128
Austria 42, 44, 49, 73, 114, 162, 177-178, 184-187, 197, 222, 275-276, 278, 280, 289
AVMSD (Audiovisual Media Services Directive) 84, 86, 140, 145-146, 148, 224, 274-275
Bangemann Report 13, 19, 80
BBFC (British Board of Film Classification) 147
behavioural inhibition 66
Belgium 49, 52, 73, 185-187, 194, 196-197, 222
Bertelsmann Foundation 29, 41
'Best interests' principle 307
Better Internet for Children 9, 14, 32, 78, 87-88, 93, 188, 206, 303-304, 307, 312, 315
Better regulation 111, 133, 135-136
Blacklisting 27
blocking access 51
blocking systems 52, 141
Brazil 117
Bulgaria 50, 73, 161, 184-186, 197, 222, 239, 289, 291
Bullying 16, 64, 70, 100, 121, 123, 125, 167, 180, 197, 227, 253-259, 268, 305
Canada 144, 241
Censorship 28, 39, 80, 85, 96, 102, 241, 273
CEO Coalition 15, 19, 32, 101, 107, 155, 157, 171
Child abuse 13, 19, 40, 44-49, 51-54, 155
child abuse imagery 48-49, 52
child abuse material 13, 19, 45-47, 52-53, 155
child online safety 14, 96, 174
Child pornography 41, 46, 48, 51-53, 87, 141, 154, 158, 178, 183-184, 227, 241
child rights 18, 98, 107, 301
child safety 15, 18, 29, 52, 96, 118, 121-122, 164, 174, 176, 182, 207
child-as-victim 95, 227
Childhood 59, 72, 74, 228-230, 234, 249-250, 262, 302, 315
Childnet International 42, 178, 187
INDEX


Children's Online Privacy Protection Act (COPPA) 163

Children’s participatory rights 302, 309

Children's Rights 15, 18, 27, 31, 84, 105, 176, 183, 227-228, 259, 262-263, 291, 301-302, 309, 312, 314, 316

China 155, 164

CIRCAMP 49, 51, 53, 181, 190

Civil society 11, 18, 39, 77, 102, 118, 146, 162, 166, 169, 173-174, 179, 181, 184, 187-191


CoE, see Council of Europe

Cognitive psychology 62-63

Command-and-control regulation 77-78, 81

Connecting Europe Facility 16


Content classification 17, 19, 23, 32, 34, 39, 88, 120, 140, 155, 287

content labeling 181

Content Regulation 134, 139-141, 250-251

Convention on the Elimination of Discrimination Against Women (CEDAW) 316

Convention on the Rights of Persons with Disabilities (CRPD) 316

Convergence 16, 27, 81, 115, 140, 148, 171, 219

Co-Regulation 15, 77-78, 81, 84-86, 88, 111, 118, 121, 126, 137, 141, 148, 155-156, 160, 223-224

Corporate social responsibility (CSR) 16, 18, 114-115, 117, 153, 159-160, 166, 188-189

Council of Europe 83, 87, 233

Council of the European Union 24, 40-41, 83, 203

Council Recommendation 231, 233, 242-243

Curriculum 153, 194, 196, 198, 202, 205-206

cyberbullying 13, 42, 74, 107, 125, 167, 180, 197-200, 227, 305, 314

Cyprus 73, 184-187, 197, 220-222, 289

Czech Republic 44, 73, 123, 177, 184, 187, 222, 290-291

Data Protection 80, 87, 140, 143-144, 148, 274, 276-277

Denmark 33, 44, 50, 53, 58, 73, 123, 177, 184-187, 194, 196, 214, 222, 288, 290, 292

Deutsche Telecom Online Service 29

DG Information Society 26-27, 57

Digital Agenda 9, 13, 16, 23, 31, 160, 203

Digital Agenda for Europe 13, 16, 160, 203

digital competence 193, 202-206, 245, 254, 261, 271-272

digital literacy skills 202, 205-206


Disney 28, 191

dopaminergic system 71

EACEA (Education, Audiovisual and Culture Executive Agency) 196, 207

EC Safer Internet programme 19, 23, 93, 97

E-Commerce Directive 41, 51, 158
INDEX

ECPAT 177, 179, 183, 190
Education sector 57, 183
ELSPA, Entertainment Leisure Software Publishers Association 115
eNACSO (the European NGO Alliance for Child Safety Online) 174, 176-179, 181, 183-184, 188, 190
Enforcement 11, 39, 41, 43-45, 47-48, 51, 58, 77, 79-80, 82, 85, 87-88, 93, 111, 114, 116, 125, 135, 137, 139, 148, 156, 159, 181, 190, 305
ENISA 198, 200
Estonia 50, 73, 177, 184-187, 214, 222, 290-292
Eurobarometer 34, 49, 58, 148, 223
EuroISPA (European Internet Service Providers Association) 48, 51, 83
Europe, internet safety awareness centres 14
European Charter of Fundamental Rights 31
European Council 24, 80, 171, 234
European Economic and Social Committee (EESC) 27, 29
European Economic Area (EEA) 12, 24, 34-35
European Framework for Safer Mobile Use 19, 84, 87, 113, 122, 125-126
European Framework for Safer Mobile Use by Young Teenagers and Children 113
European Parliament 12, 24-25, 35, 80, 84, 171, 180, 183-184, 228, 232-233, 274, 314
Europol 24, 183
Eurydice 196, 198, 200, 207
evidence base 9, 94, 97-98, 102, 146, 285
evidence-based policy 104-105, 107
Facebook 46, 53, 128, 143-144, 149, 157, 188-189, 268, 277, 287
FCC (Federal Communications Commission) 137
Film Classification 24, 147
filtering software 24, 32, 95, 244
Finland 50, 73, 114, 136, 161, 177, 184, 187, 191, 194, 214, 221-222, 288, 290
Focusing effect 63
FOSI (Family Online Safety Institute) 29 112, 180, 189-191
France 44, 73, 157, 177-178, 184-187, 191, 194, 221-222
freedom of expression 24, 29, 52, 80, 85, 88, 96, 138, 274, 301-302, 304, 306-313, 315
German Youth Protection System 134
Germany 32, 41-42, 44, 50, 73, 113, 117, 127, 140, 149, 177, 184-187, 194, 197, 200, 214, 222, 276, 289, 291-292
Greece 73, 116, 177, 184-187, 194-195, 197, 221-222, 289, 291
GSMA 19, 44-45, 87, 124, 190

323
INDEX

Labelling 24-26, 28-29, 83, 86, 112, 119, 138, 140
Larry Flynt Productions 29
Law enforcement 11, 24, 39, 41, 43-45, 47-48, 51, 58, 93, 119, 122, 181, 190
Legislation 13, 28, 39-40, 46, 78, 86, 96, 112, 114, 116, 118, 124, 126, 135-137, 143-144, 146, 148,
162-163, 165, 170, 173, 183, 260, 267, 273, 279, 312
Legitimacy 70, 79, 82, 85, 111, 173
lifelong learning 203, 206
Liikanen, Erkkii 27
Lithuania 44, 73, 114, 177, 197, 222, 239, 289-291
Luxembourg 177, 184, 187

Malta 184
McAfee 30
media environment 78-79, 133-134, 139-140, 145, 147-148, 211, 278
Media Literacy 31, 134, 139-140, 145-146, 148, 165, 193-194, 203, 220, 243, 250, 260, 264, 286
Media Regulator 18, 133-134, 136, 138-139, 141, 145, 147-148
MEDIAPPRO 58, 93
Mediation 32-33, 195-196, 211-219, 221, 223, 237, 239, 252-253, 260, 262, 267, 271-273, 279, 284-
285, 287
Microsoft 29, 113, 115, 167, 188, 191
minors, protection of 12, 17, 27, 40, 47, 49, 51, 78, 80-81, 83-87, 113, 120-121, 123, 125, 133-134,
mobile technologies 14, 112, 183
Monitoring 32, 77, 87-88, 114, 117, 121-122, 124-125, 134, 140-142, 156-158, 212-214, 252, 271-
272, 277, 279, 302
Monitoring content 158
multi-stakeholder 11, 15-16, 18, 96, 104, 101, 107, 148, 153, 180, 190, 260, 279

National Centre for Missing and Exploited Children (NCMEC) 42
Negative user generated content 69
Netherlands 41, 49, 73, 114-115, 123-124, 126-128, 147, 177, 194, 184, 187, 194, 197, 222, 288, 290
Netscape navigator 29
Neurobiology 62, 71-72
NGO Global Network 173
NICAM (Netherlands Institute for the Classification of Audiovisual Media) 115, 147
Nintendo 113, 115
Non-governmental organizations (NGO) 15, 30, 42-43, 58, 60-61, 107, 111, 122-123, 153, 166-168,
170, 173-176, 180-191, 288, 316
Nordic 33, 65, 253, 288-293, 297-298
Norway 14, 33-34, 41, 43, 53, 58, 73, 110, 161, 167, 184-187, 194, 196, 200, 214, 222, 288, 290, 292
Notice and take down (NTD) 27, 41, 45, 48, 158

Objective 12, 26, 57, 78, 80, 83, 87, 105, 115, 137, 168, 188, 191, 194, 202, 233-236, 273-274, 285,
287, 312, 314
OECD 134, 142-143, 203, 205-206
Ofcom 133-134, 136, 140, 145-146, 149
online child safety 15, 118, 164
online grooming 16, 180, 198, 200
online opportunities, children's 11, 93, 107, 211, 228, 264
online pornography 102, 107, 260
online privacy 96, 143, 163, 267
online risk 12, 19, 23-24, 32-33, 62-63, 68, 73, 98, 100, 103, 118, 126, 169, 194, 212, 214-215, 220,
223, 229-230, 237, 244, 251-259, 261, 263, 267, 271-273, 279, 291, 293-294, 297-298, 305, 314
online risk factors 100, 263, 294


online safety education 194, 197-200

Pan European Gaming Information (PEGI) 13, 25, 27, 112-117, 125-127, 179, 181


parental mediation strategies 211, 223, 271


PISA (Programme for International Student Assessment) 206

Playboy Enterprises Inc 29

Policing efforts 49

policy pillars 17

Policymaking 96-98, 103, 190, 212, 221, 223, 260, 304, 315

Pornography 29, 32-33, 41, 46, 48, 50-52, 63, 87, 95, 98, 102, 121, 139, 141, 154, 158, 178, 183-184, 227, 250, 260

Portugal 73, 177, 184-186, 200, 221-222, 253, 289, 291-292

Press Freedom 184-187, 291-292

Principles for the Safer Use of Connected Devices and Online Services by Children and Young People in the EU 87, 157

Privacy 12, 23, 27, 96, 112, 120-121, 134, 140, 142-144, 157, 159-160, 163, 167, 197-198, 201, 204, 259, 267-275, 277, 279, 297, 301, 308


Protection of Minors and Human Dignity 12, 40, 49, 51, 83, 85, 87, 193, 231, 233

Protégeles 178

Provision 16, 18, 88, 94-95, 117, 124, 140, 171, 194, 196-198, 201, 228-229, 263, 270, 279, 301-303, 307-308, 310, 315

Public consultation 121-122, 146

Public Policy 17, 77-78, 82, 94, 99, 104, 133, 136-138

Reding, Vivian 85, 116, 122, 133, 135


Regulators 133-135, 137-139, 145-148, 163, 171

regulatory authorities 17, 27, 122, 136, 145-146, 148

regulatory traditionalists 79-80

Reporters Without Borders 184, 186

reporting tools 88, 157, 162


Restriction 28, 139, 170, 214-215, 239-240, 312

Restrictions 13, 16, 45, 80, 96, 138-139, 154, 231, 238, 252-253, 277, 303, 306-307, 309

restrictive parental mediation 237

Right of access to information, Article 17 UNCRC 77-78, 241, 267, 274, 301-302, 304, 306, 309-313, 315

Right to be heard, Article 12 UNCRC 139, 228, 274, 301-307, 310-311, 313, 315
INDEX

Right to freedom of expression, Article 13 UNCRC 80, 274, 301-302, 304, 306-311, 313, 315
Risk assessment 62, 66, 202
Risk perception/perception of risk 63-64, 73
Role of the media, Article 17 UNCRC 133-134, 139, 309, 311, 315
Romania 177, 184, 194-195, 197, 221-222, 239, 289, 291
RSACi (Recreational Software Advisory Council on the Internet) 28-29
Russia 14, 42, 177
Safer Internet Action Plan 26, 34, 39, 47, 137, 180, 232
Safer Internet Awareness Centres 174, 183
Safer Internet Centres (SICs) 14, 16, 42, 49, 175, 197, 220
Safer Internet Day 14, 58, 166, 222
Safer Internet Plus Programme 24, 180, 234-236, 240
Safer Internet Programme 11, 13-16, 23-24, 42, 49, 51, 57, 62, 93, 97, 112, 166, 180-183, 185-191, 193, 228, 233, 235-236
Safer Social Networking Principles 34, 84, 87, 117, 119, 126, 156, 279
safety awareness 14-15, 58, 218, 291, 298
Safety Awareness, Facts & Tools (SAFT) project 14, 33-34, 42, 53, 58, 93
Safety Net Foundation 178
safety skills 66, 204, 207, 237, 290-291, 294, 297
Save the Children 41, 44, 177, 179, 190
Schools 9, 14, 50, 59, 100, 155, 193-195, 198-202, 204-207, 221, 237, 279, 289-290, 293, 297-298, 305
self-regulatory approaches 84
self-regulatory frameworks 147
self-regulatory schemes 17, 112, 134, 137, 147
 Sexting 47, 123, 197, 201, 255-257, 259, 268-269
Sexual abuse material 31, 39, 45-46, 48, 51, 53
Sexual exploitation 41, 49, 51-53, 87, 89, 183-184, 312, 317
Sexual images 39, 69, 74, 102, 239, 251, 253-255, 257-259, 270
Simsafety 221
Slovakia 187
Slovenia 50, 73, 184-187, 194, 197, 222, 253, 290-291
social networking 13-14, 44, 46, 84, 87, 94, 112-113, 117-119, 125-126, 156, 159, 182, 198, 200-201, 204, 213, 238, 268-270, 272, 279, 287
Social networking services (SNS) 94, 98, 113, 117-121, 126, 238, 268-270, 276-279
social networking sites 118, 125, 159, 198, 200-201, 213, 268, 287
Sony 113, 115
South Africa 117
Spain 50, 73, 161-162, 177-178, 184-187, 221-222, 291

327
INDEX

state regulation 71, 79, 85
States parties 229, 301-303, 306-307, 310-313, 316
Television Without Frontiers (TWF) 40, 84, 138, 145
the International Centre for the Missing and Exploited Children (ICMEC) 46, 179, 190
The International Classification of Nonprofit Organizations (ICNPO) 177-179
dependent Social Networking Principles for the EU (SSNP) 84, 87, 117-121, 126
teachers 59, 133-134, 139-141, 145, 147, 154, 162, 237
developmental media 78-80, 85-87
Transparency 16, 82, 85, 111-112, 122, 124, 147, 176, 188-190
Turkey 73, 177, 221-222, 239, 289-291

Ukraine 177
UNESCO 42, 197, 206
UNICEF 39, 183, 190, 278, 301
United Kingdom 51, 136, 145, 149, 194-195, 201
United States of America (USA) 119, 159
US Software Publishers Association 28
US Supreme Court 33
User-generated content 148

Vice-President Kroes 15, 30-31
Video Games 13, 28, 83-84, 113, 124, 230
violence 28-29, 46, 53, 114, 121, 137-139, 141, 230, 260

W3C (World Wide Web Consortium) 154
Webwasher 30
Welfare State 33, 253
World Wide Web Safe Surfing Project (3W3S) 30
WSIS (World Summit on the Information Society) 179-180, 188

youth protection policy 14
The Contributors

ELENA ARISTODEMOU is the head of the New Media Lab of the Cyprus Neuroscience and Technology Institute that participates in the EU Kids online network. The Lab heads CyberEthics, the Cyprus Safer Internet Center and coordinates numerous other safer internet related projects, which investigate the dangers and the perceptions about dangers in Web 3.0 environments such as Second Life; InetRisks, SimSafety, IDentifEYE. Elena has a BSc in Psychology and an MSc in Psychological Research Methods. Her interests revolve around learning disabilities and cognitive processes, research project design and statistical analysis. She is currently the coordinator of and of e-Hoop, a project focused on unifying learning differences. E-mail: elena@cnti.org.cy

MONICA BARBOVSCHI, PhD in Sociology, is a Postdoctoral Fellow at the Institute for Research of Children, Youth and Family at Masaryk University in Brno, Czech Republic, and an Associated Researcher at the Institute of Sociology of the Romanian Academy. Her research interests are at the intersection between sociology of childhood and children’s rights, and are currently materialised into European projects related to children’s internet and mobile internet use (she is the contact person for Romania in EU Kids Online and member in the Romanian team of Net Children Go Mobile). E-mail: monica.barbovschi@mail.muni.cz

WIM BEKKERS is Director of NICAM, the Netherlands Institute for the Classification of Audiovisual Media. NICAM was set up by the Dutch public and private broadcasting companies and the cinema film, DVD and game sectors. NICAM introduced Kijkwijzer, a uniform cross media classification system. NICAM is also the Administrator of the Pan-European Game Information system (PEGI). Before joining NICAM, Wim Bekkers has managed the departments for Audience Research and Documentation and Library of the Netherlands Public Service Broadcasting Organisation. He was President of the EBU Group of European Audience Researchers and also Lecturer at the University of Nijmegen. E-mail: bekkers@nicam.cc

ANDREA DUERAGER is a Lecturer and Doctoral Student at the Department of Communication, University of Salzburg, Austria. Her thesis is about children’s television in Austria, more specifically about the children’s use of television in Austria. Her main research interests are media and reception studies, especially
regarding children and adolescents, but also higher education research. She is part of the EU Kids Online Team Austria. E-mail: andrea.duerager@sbg.ac.at

SONJA DUERAGER, Dr, is Attorney-at-Law with the Austrian law firm bpv Hügel since 2007 and heads the IP-/IT Department. Her main areas of expertise are IT Law including Data Protection Law, Trademark and Copyright Law. She coordinates several workshops (e.g. of the Computer Measurement Group), and lectures on Information and Media Law at the University of Vienna and at the Media Academy for Journalists. Sonja Duerager is the author of several essays and articles in IT/IP-law matters. E-mail: sonja.duerager@bpv-huegel.com

JOS DE HAAN, Dr, is head of the research group Care, Emancipation and Time Use at the Netherlands Institute of Social Research (SCP) and professor of ICT, Culture and Knowledge Society at the Erasmus University, Rotterdam (EUR). He obtained his PhD in sociology from Utrecht University (thesis: Research Groups in Dutch Sociology) and has worked since 1994 with the SCP in the Hague, the Netherlands, where he carries out research dealing with culture, media and ICTs. E-mail: j.de.haan@scp.nl

LEEN D’HAENENS, PhD, Political and Social Sciences, University of Ghent, Belgium, is Full Professor at the Faculty of Social Sciences, Institute for Media Studies, KU Leuven, Belgium. She holds an MA in Romance Languages, an MSc in Press and Communication Sciences (University of Ghent), and an MSc in Information Studies (University of Toronto). Her current areas of research include journalism studies (frame analyses on Islam and Muslims in the news, longitudinal studies on news diversity), media and ethnic minorities (e.g., ethnic discussion forums as a source of social capital for ethnic minorities), digital media and youngsters, and media governance and accountability mechanisms. E-mail: leen.dhaenens@soc.kuleuven.be

UWE HASEBRINK, Dr, is the Director of the Hans Bredow Institute for Media Research and Full Professor for empirical communication research at the University of Hamburg. He has been a member of the EU Kids Online research network since 2006. His research fields are: patterns of media use and media repertoires, media convergence from the users’ perspective, consequences of online media for established media, media use of children and young people, forms of user interest vis-à-vis the media as well as European media and European audiences. E-mail: u.hasebrink@hans-bredow-institut.de

JØRGEN KIRKSÆTHER holds an MA in Film Science and a BSc in Computer Science. He has a diverse professional background, ranging from governmental agencies and international policy work to media production and journalism. He
is currently employed by the University of Oslo as an adviser, and is simultaneously working on finalising his PhD dissertation on sex in videogames. His main research interests are videogame history and aesthetics, censorship, and digital rights and policies. E-mail: post@transistor.no

NEELIE KROES worked in Dutch politics from 1971 to 1989, including as minister responsible for postal and telephone sectors. Subsequently, she worked on various company boards. In 1991 she became chairperson of Nyenrode University. In 2004, she became the EU’s Competition Commissioner, and, in 2010, Vice President of the Commission responsible for the Digital Agenda.

YIANNIS LAOURIS, PhD, is Senior Scientist and Chair of the Cyprus Neuroscience-Technology Institute and Director of the Cyprus Safer Internet Center. He is involved in research and applications of broadband technologies as tools to bridge the digital, economic educational and inter-personal divides. Laouris is also a pioneer in the application of the Structured Dialogic Design process. He has published several papers in peer-reviewed journals, spanning the fields of neuro-science, applied systems science, children and IT and the neuroscience of learning. He has also contributed chapters to several books and has delivered numerous presentations at national and international conferences. E-mail: laouris@cnti.org.cy”

SONIA LIVINGSTONE, DPhil, is a Professor in the Department of Media and Communications at LSE, London, and author or editor of seventeen books including, most recently, Children, Risk and Safety Online (edited, with Leslie Haddon and Anke Görzig, 2012), Media Regulation (with Peter Lunt, 2012), and Meanings of Audiences (edited, with Richard Butsch, 2013). Taking a comparative, critical and contextualised approach, Sonia’s research examines the opportunities and risks afforded by digital and online technologies in a range of contexts. She directs a 33-country network, EU Kids Online, funded by the EC’s Safer Internet Programme, and serves on the Executive Board of the UK’s Council for Child Internet Safety, for which she is the Evidence Champion. E-mail: s.livingstone@lse.ac.uk

BOJANA LOBE, Assistant Professor, has been working at the Faculty of Social Sciences, University of Ljubljana (UL) since 2002, lecturing courses such as Methodology of the Social Sciences, New Technologies in Social Science Methodology, Statistics, Integration of Qualitative and Quantitative Methods, Comparative Methods, Questionnaire Design. She has been a leading researcher on Slovenia’s largest project about children’s usage of internet in Slovenia since 2009 – Mladi na netu (www.mladinanetu.si). She has been actively working with EU Kids Online since 2005 and led methodological work packages in EU
THE CONTRIBUTORS

Kids Online I and II. She is a member of the research programme Social Science Methodology, Statistics and Informatics. She is also an associate researcher at Universite Catholique de Louvain, Belgium. She was a member of the MEDIA Expert Group of the European Commission. E-mail: bojana.lobe@fdv.uni-lj.si

MIKLÓS PÉTER MÁDER, PhD, is a Business Development Manager working for Magyar Telekom, Hungary’s leading telecom company. As an innovation expert, he is involved in numerous projects, such as EIT ICT Labs, Future Internet Platform, R&D boards. He earned a PhD in mathematical-statistics at ELTE University, Budapest. His research topics are related to ICT trends, corporate responsibility and business opportunities. E-mail: mader.miklos.peter@telekom.hu

SHARON MCLAUGHLIN, PhD, is a Law Lecturer in the Department of Law and Humanities at Letterkenny Institute of Technology Ireland. Sharon’s research focuses on communications law and policy. She was awarded her PhD from the School of Law at the National University of Ireland Galway (NUIG) for her thesis, entitled The Protection of Children in the Online and New Audiovisual Services Environment. She holds a BA in Public and Social Policy (2001), a LLB (2003) and a LLM in Public Law (2006). She is also a member of the EU Kids Online Ireland team. E-mail: sharon.mclaughlin@lyit.ie

VALENTINA MARINESCU, PhD in Sociology (University of Bucharest) is Associate Professor at the University of Bucharest – Faculty of Sociology and Social Work. She teaches undergraduate and graduate courses in media and society, and methods of researching mass communication. Her interests lie in media and communication studies in Eastern Europe, particularly in Romania. She was a fellow of Universite de Montreal (Canada), University of British Columbia (Canada) and Academy of Korean Studies (South Korea). She has also published articles and book chapters on these subject areas. E-mail: valentina.marinescu@yahoo.com

GIOVANNA MASCHERONI, PhD, is a Lecturer in Sociology of Communication and Culture in the Department of Sociology, Università Cattolica del Sacro Cuore. She is the project director of Net Children Go Mobile and principal investigator – with Cristian Vaccari and Lorenzo Mosca – of WebPolEU: Comparing Social Media and Political Participation across EU. She is a senior researcher at OssCom, Research Centre on Media and Communication based at Università Cattolica. Her research interests are devoted to: young people and the internet, use of social networking sites, online participation, digital literacy and citizenship. Her latest publications include: (2013) ‘Parenting the Mobile Internet in Italian Households: Parents’ and Children’s Discourses’, Journal of Children and Media; and (2013) ‘Performing Citizenship Online: Identity, Subactivism and Participation’, Observatorio. E-mail: giovanna.mascheroni@unicatt.it
M aria Francesca Murru, PhD, is a Post-Doctoral researcher at the Catholic University of Milan, Faculty of Political Sciences. She is currently working as a researcher at OssCom, Research Centre on Media and Communication based at the same university. Her research fields include media and children, and civic participation in online public spheres. Recent publications include: (2013) ‘The Intersection between “obvious” and “catalyzed public” through the mediating domain of civic cultures’, Journal Comunicação e Sociedade [Communication and Society]; Livingstone, S., Mascheroni, G., Murru, M.F. (2011), Utilisation des réseaux socionumériques par les jeunes européens, Hermès – Ces réseaux numériques dits sociaux, N. 59. E-mail: maria.murru@unicatt.it

Kj artan Ólafsson is a Lecturer at the University of Akureyri in Iceland and Assistant Professor at Masaryk University in the Czech Republic teaching primarily research methods and quantitative data analysis. He played a key role in the design and implementation of the 2010 EU Kids Online study and has also been involved in several other cross-national comparative projects on children’s media use, such as Net Children Go Mobile and EU NET ADB. E-mail: kjartan@unak.is

B rian O’Neill, PhD, is Head of the School of Media at Dublin Institute of Technology, Ireland. His research interests include media literacy policy and education, especially related to children and youth. He is a member of the Management Committee of COST Action ISO906 Transforming Audiences, Transforming Societies and former Chair of the International Association for Media and Communication Research (IAMCR) Audience Section. He leads the policy work package for EU Kids Online (EC Safer Internet Programme) and is also a member of Ireland’s Internet Safety Advisory Council. In 2012 he was awarded a Government of Ireland Senior Research Fellowship to research children use of ICTs and implications for national digital strategy (www.digitallyouth.ie). E-mail: brian.oneill@dit.ie

Ingrid Paus-Hasebrink, Dr, is Dean of the Faculty of Cultural and Social Sciences at the University of Salzburg, Austria, and Professor of Audiovisual Communication at the Department of Communication (responsible for the programme Audiovisual and Online-Communication). Currently she is head of a research project on media socialisation of children in socially disadvantaged environmental settings, conducted as a longitudinal study since 2005 and head of the EU Kids Online Austria Team. E-mail: ingrid.paus-hasebrink@sbg.ac.at

R emco Pijpers is Director of the Dutch foundation Mijn Kind Online (My Child Online). He has published several books about youth and media and is a well-known speaker in both the Netherlands and abroad. He is involved in the working group Positive Content (POSCON) for the European Commission. In
the Netherlands he is responsible for the positive content-competition Gouden Apenstaart (www.goudenapenstaart.nl). He majored in Journalism and History at the University of Utrecht. E-mail: remco@mijnkindonline.nl

BENCE SÁGVÁRI, PhD, is a Research Fellow at the Hungarian Academy of Sciences Centre for Social Sciences and at the International Business School, Budapest, Hungary. In addition to academic research, he is also founder and managing director of the research and consultancy firm ITHAKA, the Hungarian member of the EU Kids Online network. He holds a PhD in Sociology from ELTE University, Budapest. His research and writing primarily deals with media and internet use of children and young people, and the sociology of values. E-mail: bence.sagvari@ithaka.hu

ELISABETH STAKSRUD, PhD, is Associate Professor and Head of Studies at the Department of Media and Communication, University of Oslo. Her key research interests lie in two interlinked fields: research on Internet censorship and the regulation of content, and children and online risk. She has lead several international projects on online safety and leads the dissemination work package for EU Kids Online. She is a widely used public lecturer, with several publications, most recently Children in the Online world: Risk, Regulation, Rights (Ashgate, 2013). She is a former Harvard Berkman Center Fellow, and a former officially appointed ICT adviser to the Norwegian minister of government administration and reform. E-mail: elisabeth.staksrud@media.uio.no

TATJANA TARASZOW is a PhD Candidate at the Humboldt-Universität zu Berlin. Her research interests focus on language acquisition, migration, as well as on interculturalism, intercultural communication, and conflict resolution. She received her Master’s degree (MSc) in psychology with emphasis on media and educational psychology from the University of Tübingen (Germany) and McGill University (Canada). Her previous work included coordinating EU and UN co-funded projects focusing on safer internet, mobile learning, and interculturalism as well as development of a mobile app for second-language acquisition with an NGO based in Cyprus. Tatjana is facilitator of SDDSM and mediator. E-mail: tatjana.taraszow@hu-berlin.de

LIZA TSALIKI, PhD, is Assistant Professor at the Faculty of Communication and Mass Media at the National and Kapodistrian University of Athens, and a Visiting Senior Fellow at the London School of Economics. Her recent research interests include the sexualisation of children debate; children with disabilities; pornography; social media; celebrity culture; audiences. For more details and a publication record, visit http://www2.media.uoa.gr/people/tsaliki/. E-mail: etsaliki@media.uoa.gr
SIMONE VAN DER HOF, Dr, is Full Professor of Law and Information Society and Head of the Center for Law and the Information Society of Leiden Law School at Leiden University. Simone’s research concentrates on the impact of new technologies on individuals and their rights. Current research topics include: online privacy, data protection and privacy statements, digital identities, digital child rights, (legal, social, technological) regulation of online child safety and empowerment of individuals through technology. E-mail: s.van.der.hof@law.leidenuniv.nl
Director and Administration

Director: Ulla Carlsson
Telephone: +46 31 786 12 19
Fax: +46 31 786 46 55
ulla.carlsson@nordicom.gu.se

Technical Editing and Webmaster:
Per Nilsson
Telephone: +46 31 786 46 54
Fax: +46 31 786 46 55
per.nilsson@nordicom.gu.se

Field of Activities

Nordic Media Trends
Nordic Co-ordinator: Eva Harrie
Telephone: +46 31 786 46 58
Fax: +46 31 786 46 55
eva.harrie@nordicom.gu.se

Nordic Media Policy
Editor: Terje Flisen
terjef@nordicmedia.info

Outlook Europe & International
Editor: Anna Celsing
anna.celsing@skynet.be

The International Clearinghouse on Children, Youth and Media
Scientific Co-ordinator:
Cecilia von Feilitzen
Telephone: +46 8 608 48 58
Fax: +46 8 608 41 00
cecilia.von.feilitzen@sh.se

Information Co-ordinator:
Catharina Bucht
Telephone: +46 31 786 49 53
Fax: +46 31 786 46 55
catharina.bucht@nordicom.gu.se

National Centres

Nordicom-Denmark
State and University Library
Universitetsparken
DK-8000 Aarhus C, Denmark

Media and Communication Research
Maria Hvid Stenalt
Telephone: +45 89 46 21 67
Fax: +45 89 46 20 50
mhs@statsbiblioteket.dk

Nordicom-Finland
University of Tampere
FI-33014 Tampere, Finland

Media and Communication Research
Päivi Lukin
Telephone: +358 3 3551 70 45
Fax: +358 3 3551 62 48
paivi.lukin@uta.fi

Nordicom-Norway
Department of Information Science and Media Studies
University of Bergen
PO Box 7800
NO-5002 Bergen, Norway

Media and Communication Research
Ragnhild Molster
Telephone: +47 55 58 91 40
Fax: +47 55 58 91 49
ragnhild.molster@infomedia.uib.no

Media Trends and Media Statistics
MediaNorway
Nina Bjørnstad
Telephone: +47 55 58 91 26
Fax: +47 55 58 91 49
nina.bjørnstad@infomedia.uib.no

Nordicom-Sweden
University of Gothenburg
PO Box 713
SE-405 30 Göteborg, Sweden

Media and Communication Research
Roger Palmqvist
Telephone: +46 31 786 12 20
roger.palmqvist@nordicom.gu.se

Karin Poulsen
Telephone: +46 31 786 44 19
karin.poulsen@nordicom.gu.se

Media Trends and Media Statistics in Sweden
Ulrika Facht
Telephone: +46 31 786 13 06
ulrika.facht@nordicom.gu.se

Karin Hellingwerf
Telephone: +46 31 786 19 92
karin.hellingwerf@nordicom.gu.se

Staffan Sundin
Telephone: +46 36 16 45 82
staffan.sundin@nordicom.gu.se
Keeping children safe online has been the subject of intensive policy debate ever since the mid-1990s when the internet first became an important public communications medium. The European Union has been to the fore in promoting internet safety and through its Safer Internet Programme has supported multi-stakeholder initiatives with industry, law enforcement, education and civil society to create a safer internet environment. Now, with a new emphasis on not just a safer but also a better internet, policy makers have signalled a new phase in strategies to protect children online. Reviewing the development of internet safety policy over this period – against the background of better evidence about the reality of young people’s experiences – and looking to its future are among the key themes of this book.

Contributors, all members of the now 33-country EU Kids Online network, seek to add to a growing literature on policy matters regarding internet regulation and governance as the Internet enters a new phase of maturity with near universal access and use. European in scope but international in outlook, the chapters in this collection seek to raise critical debate on just how mainstream are policies to protect young people, promote their best interests online and empower them to avail of the full range of digital opportunities? Against a background of increased international tension and debate over whether the internet should be regulated at all, contributors adopt a somewhat different position and assess the forms, contexts and evidence in favour of action – regulatory and otherwise – needed to support safer and better outcomes for young people.