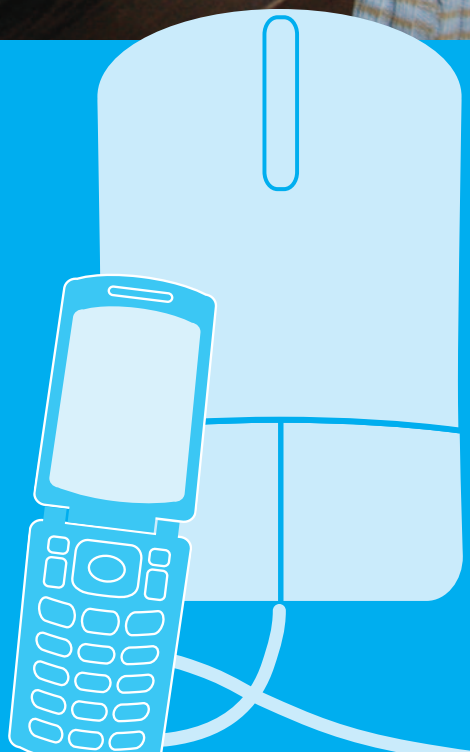
UNICEF
Innocenti Research Centre

Child Safety Online

Global challenges and strategies



unicef
unite for children

THE UNICEF OFFICE OF RESEARCH, INNOCENTI

The Innocenti Research Centre (IRC) was established in Florence, Italy in 1988 to strengthen the research capability of the United Nations Children's Fund (UNICEF) and to support its advocacy for children worldwide. The Centre helps to identify and research current and future areas of UNICEF's work. Its prime objectives are to improve international understanding of issues relating to children's rights and to help facilitate full implementation of the Convention on the Rights of the Child in developing, middle-income and industrialized countries.

IRC is the dedicated research hub of the UNICEF Office of Research (OOR), which provides global leadership for the organization's strategic research agenda around children. The Office aims to set out a comprehensive framework for research and knowledge within the organization, in support of its global programmes and policies. Through strengthening research partnerships with leading academic institutions and development networks in both the North and South, the Office seeks to leverage additional resources and influence in support of efforts towards policy reform in favour of children.

IRC's publications are contributions to a global debate on children and child rights issues and include a wide range of opinions. For that reason, the Centre may produce publications that do not necessarily reflect UNICEF policies or approaches on some topics. The views expressed are those of the authors and/or editors and are published by the Centre in order to stimulate further dialogue on child rights.

The Centre collaborates with its host institution in Florence, the Istituto degli Innocenti, in selected areas of work. Core funding for the Centre is provided by the Government of Italy, while financial support for specific projects is also provided by other governments, international institutions and private sources, including UNICEF National Committees.

Front cover photo: © UNICEF/NYHQ2010-3011/Giacomo Pirozzi

Design and layout: BlissDesign.com

December 2011

ISBN: 978-88-6522-004-7

To access the most up-to-date publications, please go to the relevant pages on our website, at <www.unicef-irc.org/publications/>.

Correspondence should be addressed to:

UNICEF Innocenti Research Centre
Piazza SS. Annunziata, 12
50122 Florence, Italy
Tel: (39) 055 20 330
Fax: (39) 055 2033 220
florence@unicef.org
www.unicef-irc.org

Child Safety Online: Global challenges and strategies

CONTENTS

ACKNOWLEDGEMENTS

This publication, Child Safety Online: Global challenges and strategies, was coordinated by the UNICEF Office of Research, Innocenti, assisted by an international panel of advisers and reviewers. The research was conducted in close consultation and collaboration with the Child Exploitation and Online Protection Centre (CEOP) in the United Kingdom. Special thanks to the following UNICEF country offices that provided data, case studies and recommendations that informed the report: Albania, Brazil, Croatia, the Philippines, South Africa, Thailand and Venezuela (Bolivarian Republic of).

This study was made possible through a generous contribution from the Japan Committee for UNICEF.

Research

Gerison Lansdown, lead researcher; independent consultant on child rights and child participation

Margaret Akullo, criminology expert; Project Coordinator for Project Childhood: Protection Pillar, United Nations Office on Drugs and Crime, Bangkok

John Carr, expert adviser on use of the Internet and related technologies by children and young people

Mark Hecht, Legal Counsel, Children's Aid Society of Ottawa

Tink Palmer, Chief Executive Officer, Marie Collins Foundation

UNICEF Office of Research, Innocenti

Gordon Alexander, Director

Jasmina Byrne, Child Protection Specialist

Andrew Mawson, Chief of Child Protection

Susanna Nordh, Consultant

Claire Akehurst, Executive Assistant

UNICEF technical support/advice

Karin Heissler, Child Protection Specialist, Planning and Evidence-Building, UNICEF New York

Priscillia Hoveyda, Consultant, Young People, UNICEF Division of Communication, New York

Ravi Karkara, child participation specialist, formerly with the Division of Policy and Practice, UNICEF New York

Ann Linnarsson, Protection Specialist, UNICEF Port-au-Prince; former Programme Officer, IRC

Clara Sommarin, Child Protection Specialist, UNICEF New York

Child Exploitation and Online Protection Centre

Graham Ritchie, Missing and Trafficked Children Manager

Gabrielle Shaw, Head of International Relations

External advisers/peers reviewers

Alisdair A. Gillespie, Professor of Criminal Law and Justice, Department of Law, De Montfort University, Leicester, United Kingdom

David Finkelhor, Director, Crimes against Children Research Center, Co-Director, Family Research Laboratory, Department of Sociology, University of New Hampshire, United States

Ethel Quayle, COPINE Research, Clinical and Health Psychology, School of Health in Social Science, University of Edinburgh, United Kingdom

Julia Davidson, Director of Research in Criminology and Sociology; Co-Director, Centre for Abuse and Trauma Studies, Kingston University, London

Lars Lööf, Head of Children's Unit, Council of the Baltic Sea States

Lena Karlsson, Director, Child Protection Initiative, Save the Children; former Child Protection Specialist, IRC

Olga Kolpakova, Head of Prevention Programs Department, Stellit, Saint Petersburg, Russian Federation

Rodrigo Nejm, Director of Prevention Programmes, SaferNet Brasil

Sonia Livingstone, Coordinator EU Kids Online; Professor and Head of Department of Media and Communications, London School of Economics and Political Science

Tiago Tavares Nunes de Oliviera, Founder and President of SaferNet Brasil

Pia Lang, former Policy Officer, Safer Internet Programme, European Commission

Editorial

Christine Dinsmore, editing

Catherine Rutgers, copy-editing

Baishalee Nayak, fact-checking

FOREWORD

Over the past twenty years the Internet has become an integral part of our lives. We have eagerly embraced its potential for communication, entertainment and information-seeking. For many of today's children, the Internet, mobile phones and other technologies are a constant and familiar presence. For them, the distinction between online and offline has increasingly become meaningless, and they move seamlessly between both environments.

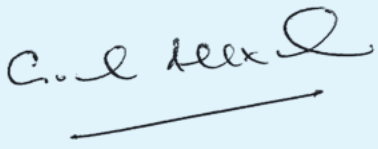
An increasing number of children can scarcely imagine life without a social networking profile; videos and photographs shared online – often in real time – and online gaming. Indeed, young people are at the vanguard of technological change. Their coming-of-age in this era of exponential innovation has widened the generational divide between them and their parents, their teachers and other caregivers. This gap, while becoming less stark in industrialized countries, is wider in lower-income countries where caregivers arguably have fewer opportunities to access information and communication technology. But the situation is changing rapidly.

There is no doubt that the Internet yields numerous opportunities and benefits for children in terms of its impact on their educational attainment and social inclusion. However, it has also exposed children to dangers that defy age, geographic location and other boundaries that are more clearly delineated in the real world. This has resulted in risks to children and young people of having abusive images of them shared on the Internet; of being groomed or lured into sexual conversations or exploitation by adult offenders; of being bullied or harassed online.

Bearing this in mind, the UNICEF Innocenti Research Centre has, in partnership with the Child Exploitation and Online Protection Centre in the United Kingdom, collaborated with a number of actors to undertake this study. The research explored children's online behaviour, risks and vulnerability to harm, documenting existing preventive and protective measures to combat their online abuse and exploitation. The study draws on lessons from high- and middle-income countries, viewed through the lens of the dynamic that, given the speed of innovation, other countries may soon experience.

What we have learned is that a singular approach to combating these crimes is not effective. What is required is a collective effort by policymakers, law enforcement agencies, social workers, teachers, parents and the private sector to systematically protect children. We have also discovered that many children are comfortable navigating the Internet and are able to avoid risks. They may see themselves as protectors of younger children and are themselves agents for change. Children should be allowed to express their views on how to mitigate risks, and they should be listened to and empowered to safely exploit the benefits of the Internet. However, we should not overestimate their ability to protect themselves. Ultimately, the onus lies with adults to put in place a framework that ensures children equal and equitable access to the Internet, along with a safer online environment.

Access to knowledge, participation, leisure and play are fundamental rights of all children, as enshrined in the Convention on the Rights of the Child. In today's real and virtual worlds, it is our collective responsibility to ensure those rights for all children.



Gordon Alexander
Director
UNICEF Office of Research, Innocenti

INTRODUCTION

The Internet, mobile phones and other electronic media provide children and young people with levels of access to information, culture, communication and entertainment impossible to imagine just twenty years ago. With many of their extraordinary benefits, however, come hazards. The Internet and associated technologies have made abusive images of children easier to create and distribute, and provide significant new opportunities for abusers to access and make contact with children and young people online. While information and communication technology (ICT) has not created crimes involving sexual abuse and exploitation of children, it has enhanced the scale and potential of some old and familiar ones.

Expanding Internet access for all children and young people without discrimination and exclusion in all parts of the world, together with promoting digital citizenship and responsibility, ought to be critical objectives for policymakers concerned with enhancing opportunities for children.[1] Building safer Internet access is integral to that project. Questions such as 'what is the nature of risk globally?' and 'what are the most effective strategies to address it?' are therefore important. The purpose of this report, which was developed by the UNICEF Innocenti Research Centre (IRC) in partnership with the Child Exploitation and Online Protection Centre (CEOP), is to review the global evidence available. The study primarily addresses two issues: child sex abuse recorded in images; and the grooming of young people for sex. A third issue, cyberbullying, emerging from much research as an issue of particular significance to children, is also touched on in this report.

There are many knowledge gaps about the protection challenges raised by the Internet, particularly in parts of the world where its penetration is so far more limited. There has been significant work undertaken to analyse children's online behaviour and investments made in strategies to address and prevent abuse in parts of Asia, across Europe and the United States of America. But there has been less exploration of online child abuse and exploitation across many low- and middle-income countries, or examination of the state of knowledge and/or the responsiveness of bodies with responsibilities for child protection and law enforcement. Little research exists about the use of the Internet by children and young people in Africa, much of Asia and Latin America (and the bearing this might have on risk). Furthermore, research findings from different parts of the industrialized world are sometimes contradictory.

It would be a mistake to believe that child abuse in which ICT plays a role is only an issue for the economically better off, whether societies or social groups. Web access is rapidly expanding, supported by increasing broadband and mobile phone penetration. Indeed, the emergence of broadband has been a decisive factor in facilitating online child abuse because it allows the exchange of larger files, particularly files containing photos, videos and audio. As broadband starts to become available in lower-income countries there is a high expectation that, absent any contrary measures, patterns of abusive behaviour witnessed elsewhere will follow.

Globally, children and young people tend to become early users and prime innovators on the Internet, and are often far ahead of their parents and other adults in terms of use, skills and understanding. The Internet, particularly social networking and other interactive media, provides new forms of social space globally that did not exist when most contemporary parents were themselves children. Young people in all societies today are pioneers, occupying online spaces in ways that adults often cannot imagine. These spaces can be immensely creative, but can also expose children to dangers adults may in many instances only dimly perceive.

The ease of interaction among and with children, the risk of sexual abuse, new and fast-changing technology, and adults' lack of awareness and understanding of the Internet or children's usage, is a recipe for societal anxiety – as well as sensationalism, myth-making and potentially inappropriate policy responses. New technologies are commonly accompanied by fears as to their potential dangers, often provoked without a solid foundation in

evidence. The popular fear that the Internet endangers all children has not been supported by the research evidence so far.[2] Nevertheless, there are genuine risks associated with it, and calibrating appropriate protective responses requires reliable information that helps to accurately identify the nature and scale of risk and harm.

Although much of the original research and work that led to the development of the Internet involved both public and private sector partners, since the mid-1990s the Internet has been recognized as being owned and driven almost entirely by private sector entities. Meanwhile, it has become central to the global economy and, by extension, to the efficient functioning of a great many and rapidly increasing number of national economies. It underpins public infrastructure that provides for the smooth operation of transport, power, banking and other vital systems. It is playing a major role in the social and political lives of a substantial and growing number of citizens around the world. Precisely because of this dimension, governments, inter-governmental bodies and other public agencies have generally proceeded with circumspection when discussing new laws or regulations regarding how the Internet should operate, or what is expected of the myriad large and small companies that make up the modern Internet industry. The urge to legislate and regulate in ways that might curb the Internet is clearly there, however, as reactions by politicians to phenomena such as the use of social networking sites (SNS) during periods of civil disorder have shown.

Governments have tended to tackle online-related sexual exploitation and abuse with an emphasis on building the 'architecture' to protect or rescue children – establishing legislation, pursuing and prosecuting abusers, raising awareness, reducing access to harm and supporting children to recover from abuse or exploitation. These are essential components of a protection response. Internationally, however, progress is patchy. Many legal jurisdictions, for example, fail to enact legislation sufficient to combat child abuse images or laws to criminalize grooming. There is also a lack of awareness or discomfort among parents and agencies with child protection responsibilities about the real nature of hazards or effective protection strategies. Awareness of online-related child abuse and exploitation appears not yet to be organically embedded in the great majority of child protection systems and responses. Integrating awareness of online-related abuse and exploitation into the broader child protection agenda should be a priority for policymakers.

Given the centrality of the private sector to the Internet, it has major responsibilities in relation to child protection online. Under contemporary understanding of corporate responsibilities for respecting human rights, recently internationally articulated in the report entitled 'Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework', businesses have obligations both to respect human rights and to seek to prevent or mitigate adverse human rights impacts directly linked to their operations, products and services.[3] Child abuse and exploitation are manifestly "adverse human rights impacts." The industry has it in its powers to develop and introduce new tools to make the Internet safer for children. The importance of action by the private sector in support of law enforcement and Internet safety are discussed later in this report.

There are genuine challenges and fears within the industry. Some of the measures that could contribute to making the Internet safer for children appear to challenge current business models; they might appear to reduce the competitiveness of an individual company, or to threaten other freedoms inherent in the way the Internet currently operates. However, it is arguably in the longer-term interests of the Internet itself, and in particular of the larger companies that dominate it, for governments to feel that legitimate concerns for the welfare of their citizens, perhaps especially in relation to children and young people, are taken seriously and are acted upon promptly. Otherwise there is a risk that governments or regional bodies will step in to regulate and legislate in ways that negatively affect the Internet as a single global system embodying freedom of information.

Given that most research on usage and risk has taken place in the industrialized world, the extrapolation of findings to other socio-economic and cultural contexts must be approached with caution. However, there is enough research in low- and middle-income countries to be suggestive of patterns and potential problems. One important finding from industrialized and lower-income countries alike is the importance of action, innovation, exploration and discovery by adolescents on the Internet; in other words, the significance of child agency in accessing the creative benefits of the Internet, in exposure to certain forms of risk, and in managing that risk.

The protection response needs to strike a balance between the right to protection from all forms of violence, sexual abuse and exploitation, and the rights to information, freedom of expression and association, privacy and non-discrimination, as defined in the Convention on the Rights of the Child and other relevant international standards. That balance must be anchored in the best interests of children as a primary consideration, the right to be heard and taken seriously, and recognition of the evolving capacities of children and young people. It is unlikely ever to be possible to remove all the risks to children and young people that exist in the online environment. Moreover, beyond a certain point, attempting to do so could threaten the very essence of the Internet and its multiple benefits.

It would be a mistake ever to think that all children and young people are equally adept or at home in the online environment, or equally knowledgeable about it.[4] Children's use of the Internet and their behaviour and vulnerabilities online differ according to their age. To be effective, protection strategies need to incorporate measures and messages appropriate to different ages and levels of understanding. It is nonetheless the case that by and large children and young people are often the best experts in relation to their own ICT usage. This report argues that effective protection strategies require children's participation, particularly that of adolescents, in both their design and implementation, as well as the empowerment of parents and other adults who work closely with young people, such as teachers, to enable them to support and understand children's use of ICT and the risks and hazards that they may encounter. This is both a pragmatic recognition of reality and a position based on human rights principles.

This report discusses the nature and scale of sexual abuse and exploitation of children and young people online and the types of crimes perpetrated against them. It considers the generational divide between parents and children in their knowledge of, and engagement with, the online environment and how this affects experiences and approaches to the Internet and its usage. The report outlines how children and young people across the world use the Internet, including an examination of specific online activities and experiences that have the potential to place them at risk. There is a focus on activities that involve interaction online and offline and an analysis of research findings about where children turn for support when things go wrong.

The challenge for policymakers is not to get sidetracked into blaming the medium. Instead, it is to coordinate action by a range of public and private actors on a number of interrelated issues that ultimately come under the heading of 'building a safer Internet'. These include integrating an understanding of the methods of child sexual abuse and exploitation into building Internet access; understanding child usage of ICT and working with young people on effective safety strategies; integrating awareness and understanding of online-related child abuse and exploitation into child protection systems; developing effective law enforcement against online-related child abuse and exploitation; and integrating child protection into effective law enforcement. While usage may still be less pervasive in low- and middle-income countries, protection is a challenge they will face in the imminent future that needs to be addressed now.

The report also considers ways to build a safer environment for children and young people for whom the Internet is a basic social medium in which the online and offline worlds come together. It outlines relevant international law and key challenges to governments and law enforcement agencies in achieving greater protection for children and young people. It argues that a multitiered approach is necessary to challenge the potential threats to children's well-being and safety in the online environment. Accordingly, it concludes by putting forward a strategic protection framework with four main objectives: 1) empowering children and promoting their resilience; 2) removing impunity for abusers; 3) reducing availability of harmful material from the Internet and access to harm; and 4) promoting recovery and rehabilitation for children who have experienced harm.

© UNICEF/NYHQ2007-0269/Cirillo

PART ONE

CHILD ABUSE LINKED TO INFORMATION AND COMMUNICATION TECHNOLOGY

The nature and scale of child abuse online

A study conducted by Sonia Livingstone and Leslie Haddon of EU Kids Online, has defined a set of categories to understand risk and harm related to online activities. The groupings elucidate the features of behaviours involved and help orientate researchers and policymakers towards their different implications: a) online harm from content (the child as a passive recipient of pornographic or harmful sexual content); b) harm from contact (the child targeted as a participant by an adult or another child in activities such as sexual abuse that is photographed and then disseminated, for online grooming for sexual abuse, or for bullying); and c) harm from conduct (the child actively initiates risky or abusive behaviour, for example, by creating or uploading pornographic material, physically meeting an adult met online, placing images of her or himself or another young person online, downloading abusive images of children or bullying).[5] The range of adult behaviour that constitutes child sexual abuse online includes adults who sexually exploit their own or other children for the production of child abuse images; those who download images for their own personal use; those who create and distribute images; and those who seek access to children online in order to exploit them.

It is estimated that the number of child abuse images on the Internet runs into the millions and the number of individual children depicted is probably in the tens of thousands.[6] An important difference between an image online and one offline is that, once online, an image can remain in circulation in perpetuity and there is almost no limit on how often or by whom it can be viewed or passed on. Some currently available images are thought to have been produced more than 20 or 30 years ago, derived from film photographs or videos that have since been digitalized.[7] However, the majority of images in cyberspace have been produced much more recently and are linked to the emergence of cheap, easy-to-use digital cameras and the development of the Internet.

The majority of children featured in child abuse images currently online are Caucasian, prepubescent girls (between the ages of less than 1 and 10).[8] This preponderance may be a reflection of the fact that most research has thus far been undertaken in Western countries, and offenders demonstrate a preference for children who share their own ethnic characteristics. It may also reflect greater availability of ICT and other technologies for image capture and distribution in industrialized countries. There is an identifiable downward age trend and images are becoming more graphic and violent.[9] What is not yet clear is whether child abuse images online are a form of abuse limited to certain parts of the world, or whether they represent a stage in the progress of Internet uptake and usage. In other words, will child sex abuse recorded in images involving children from Asian or African backgrounds become more common as Internet access becomes ever more global?

It is difficult to estimate the number of websites globally that depict child abuse images. The Internet Watch Foundation (IWF) has identified

and taken action against some 16,700 instances of child sexual abuse content on different web pages worldwide in 2010 compared with identifying around 10,600 URLs of individual web pages or websites in 2006.[10] The increase may be attributed to a change in hosting patterns, whereby content is being posted to separate locations rather than multiple images being stored on a single web page.[11] Most significantly, however, child abuse images are increasingly shared among networks of like-minded individuals through peer-to-peer distribution, which avoids the necessity of housing the images on storage systems owned by third parties such as Internet service providers (ISPs).[12]

Online grooming is the process by which an individual befriends a young person for online sexual contact, sometimes with the involvement of webcams that can allow 'sharing' of the exploitation among networks of child sex abusers, and sometimes extending to a physical meeting to commit sexual abuse.[13] The areas of cyberspace that enable abusers to groom potential victims include chat rooms, social networking sites (SNS) and instant messaging.[14] Research with abusers suggests that some have up to 200 young people on their online 'friends' lists who are at different stages of the grooming process at any given time.[15] Grooming may take minutes, hours, days or months, depending on the goals and needs of the abuser and reactions of the young person.

In terms of age, the evidence suggests that the children most at risk of being groomed are adolescents, particularly adolescent girls. At this age, children are often active users of the Internet as a means of meeting people and making friends – all part of the process of developing their sense of self, including their social, sexual and emotional identities.

There is no information concerning the number of individuals (who evidence suggests are mainly men) grooming children online. In many countries, this activity is not yet a criminal offence and therefore no records are kept relating to such behaviour. Even among countries where grooming has been criminalized, there are no coordinated databases that provide details of the offenders. This represents not only a huge gap in knowledge, but also in child protection.

There are as many myths about child sexual abuse online as there are about child sexual abuse offline. One is that strangers pose the greatest threat to children. With respect to the initial creation and dissemination of child abuse images, this is false. Those directly responsible are often family members and other caregivers who have easy and private physical access to children.[16] Another myth is that grooming typically involves older men lying and forcefully entrapping innocent children by using false identities. This is also largely untrue. Rather, it tends to be a process of 'seducing' or flattering children into what the child may perceive as a voluntary sexual online friendship. Although some offenders lie about their age or gender when grooming children, the activity generally tends to fit a model of statutory rape.[17]

The available evidence, which mainly derives from studies in industrialized countries, points to a typology of child sex abusers online as mainly Caucasian, male, commonly in employment, reasonably well educated, and spanning a wide age range, including young people themselves. Many men who engage in offline sexual abuse of children also engage in abuse online. However, a significant proportion of men who view child abuse images online do not appear to seek sexual contact with children offline.[18] This finding should, however, be considered with caution. Offenders who have accessed child abuse images online have demonstrated some form of sexual interest in children, and may therefore pose a physical risk to them. At the very least, such offenders have contributed to sustaining demand for the production of images that involve the sexual abuse of children.

ICT has also created an environment in which pornography has become easily accessible. One of the key differences with the 'pre-Internet' era is that today there are many available sites displaying extreme forms of pornography that can be accessed by young people.[19] There is, to date, limited research evidence on the implications of such exposure. Concerns are increasingly expressed by professionals working with young people on apparently growing levels of addiction to pornography, as well as emerging pressures on girls to conform to both the sexual behaviours and appearances of women in pornographic videos.[20] ICT has also led to the phenomenon of exposure to unsolicited pornography. The extent to which children are disturbed by such exposure appears to be influenced by age, social norms in their country and the degree of control they have over viewing these sites.[21]

Children have reported that bullying online – cyberbullying or online harassment – is an

important issue for them. While for adults this has not been as significant a concern as sexual abuse, it is now beginning to receive more attention.[22] Bullying can be defined as a child being the target of behaviour that is harmful or intended to cause harm, occurs repeatedly, and involves an imbalance of power that prevents the victim from challenging or ending the behaviour.[23] While more bullying takes place offline than online, in Europe at least, the Internet and mobile phones now provide new and more invasive and anonymous opportunities for children and young people to bully others.[24]

The prime instigators of cyberbullying are generally other children and young people. Some studies have suggested that more girls than boys bully online; other reports suggest the reverse.[25] Research from Canada and the United Kingdom identifies children who are at risk of being bullied offline (for example, children who may be perceived as 'different', such as minority ethnic groups, lesbian, gay, bisexual or transgender (LGBT) young people, overweight children, or those with perceived disabilities) to be at greater risk of being bullied online than other children.[26] In contrast, research from the United States has found that those who physically bully others at school were themselves likely to be victims of electronic bullying.[27] Although cyberbullying does not yet appear to be a common experience, it can have a significant impact on children and young people because of its anonymity, its capacity to intrude at any time of day or night into places that might otherwise offer respite and sanctuary – homes and bedrooms – and by its nature to often extend (sometimes unwittingly) to implicate and involve many people.

Child access to the Internet

The evidence points to growing online connectivity of children and young people. To date, levels of Internet access are highest in the industrialized world, although low- and middle-income countries are fast catching up. Social inequalities affect access and usage. Both in richer countries in general, and among better-off children within all countries, access to and usage of the Internet are higher than among poorer countries and less well-off children.[28] In most countries for which data are available, children under the age of 18 make up a high percentage of the total number of people online.[29] But in Europe, the number of parents who are accessing the Internet is rapidly approaching the number of children who use it. In 2008, an average of 84 per cent of parents throughout the region had used the Internet compared with 66 per cent in 2005.[30] As evidence from a European Union (EU) study shows, as parents use the Internet more, they acquire additional Internet-related skills and are better equipped to manage their children's Internet use.[31]

Overall, there appears to be little gender difference in levels of usage. Age, though, is a relevant factor, with, in general, levels of access increasing with children's age.[32] Younger children are going online in greater numbers, however, with the age of first-time Internet use decreasing. In the EU, based on parental perceptions, 60 per cent of 6- to 10-year-olds were using the Internet in 2008, compared with 86 per cent of 15- to 17-year-olds, but this nevertheless represents an increase in access by younger children over previous years.[33] Globally, the number of children spending more time online appears to be increasing, yet there remain striking differences in the hours of usage. In Europe, for example, children aged 9 to 16 who access the Internet do so for between one and five hours each day,[34] whereas in Bahrain, the access is between two and a half and three and a half hours each day.[35] In South Africa, many Internet users go online as infrequently as once a week and then for less than an hour.[36] In Brazil, 69 per cent of children between 10 and 15 years old access the Internet every day.[37] However, the International Telecommunication Union (ITU) reports that, in terms of the frequency of use, children aged 5 to 14 are far less likely to use the Internet at least once a day (or almost every day) than the population as a whole or young people aged 15 to 24.[38] A survey of 9,000 adult and child Internet users in 12 countries, including China, India, Japan, the United Kingdom and the United States, found that parents underestimate the time their children are online – the children spend on average 39 hours per month on the Internet, twice as much time as their parents believe. This discrepancy may indicate a lack of parental engagement, supervision and communication with children. Exceptions were found in Brazil, Italy and Sweden, where there seems to be more agreement about levels of Internet usage by children among parents and children.[39]

In industrialized countries, the majority of children have access to the Internet at home or at school, whereas in lower-income countries many children rely on Internet cafes,[40] which potentially bring unknown adult and child users into the same physical space. In Brazil, for example, access to technology among children aged 10 to 15 increased from 53 per cent to 63 per cent between 2008 and 2009. Access from Internet cafes (Lan Houses), both free and paid, among Internet users of the same age group, increased from 33 per cent in 2006 to 61 per cent in 2009.[41]

The landscape of Internet usage is also changing, with mobile phones becoming a significant source of access. While in general computers remain the main mode of going online, Japan is leading the way with nearly 60 per cent of children now using their phones for access.[42] It is likely that children's use of Internet-enabled mobile devices will progressively increase based on countries' socio-economic conditions.

The global explosion of mobile phone use is highly significant. Mobile phones and mobile devices of different kinds represent the future of Internet connectivity, especially in low- and middle-income nations. It is thought unlikely that many of these countries will invest in the infrastructure necessary to install Internet-bearing telephone cables or wires that reach into every home. Rather, they will establish a network of wireless wide area networks linked to or in addition to conventional mobile phone masts. The increasing use of Internet-enabled 'smartphones' for going online will limit the ability of parents to restrict, monitor or control what their children access and therefore will increase potential risks to children and young people. Mobile phones carry with them an immediacy that simply does not exist when the device being used is in a fixed location, where supervision is easier. But even phones that are not Internet-enabled provide young people with enormous opportunities to remain in contact and, for this reason, are now seen as necessary social tools for young people in many industrialized and middle-income countries.

Children and young people are engaged in a wide range of online activities – games, information, education, entertainment and communication. The ITU reports generally higher use of the Internet by children for education and games than among other age groups, and greater use by youth and the general population for communication.[43]

Social networking sites, instant messaging, chat lines, micro-blogging platforms and other forums enable users to post and exchange personal information, photos and videos, build networks of friends, and maintain high levels of interaction and information exchange on every aspect of their daily lives.

SNS are enormously popular with young people, who increasingly view them as integral to their social lives. Studies on young people's usage and behaviour online from Australia, Bahrain, Brazil, Nepal, the Philippines, South Africa, the United States and countries in Europe, indicate that most young people who use the Internet do so in similar ways, particularly in respect of use of SNS. The studies reveal a remarkably common pattern of social activities – meeting people, making new friends and chatting online – suggesting that factors relating to child and adolescent development are more significant than cultural factors as the drivers of online communication. In the United States, 73 per cent of teenagers online now use social networking sites.[44] Across the EU, 59 per cent of 9- to 16-year-olds have a social networking profile, including 26 per cent of 9- to 10-year-olds, and 82 per cent of 15- to 16-year-olds.[45] About 5 per cent of the estimated 37 million Facebook users in India are between 13 and 15 years old, and 7 per cent are between 16 and 17 years old.[46] In Brazil, the number of Facebook users reached 29 million by October 2011, of whom 6 per cent were between 13 and 15 years old and 7 per cent were between 16 and 17 years old.[47]

Social implications of the merged online/offline environment

A key dimension of the growth of online activity is that children and young people are participating in, learning from, and creating an environment that, in many parts of the world, still remains unknown and unfamiliar to their parents. Growing numbers of children are now creating and exploring their own virtual social networks. Through online advertising, through exposure to knowledge and information, and to political, religious, cultural or sexual ideas that may be profoundly at odds with those of their parents, their worlds today are significantly more complex. There are also concerns that greater access and exposure to electronic media can have harmful implications, including

potentially diminishing parental capacity to understand children's experiences or to offer effective protection and support.[48] While the generational divide around Internet usage is beginning to narrow in the industrialized world, the gulf between children and parents in Internet use in lower-income countries remains significant.

The online environment allows for a complex mix of individual anonymity, self-promotion and role-playing according to the wishes and whims of the user. Children and young people can define their own online identities, can change those identities and can inhabit several different ones at any given time. It adds a new dimension to social interaction and a new form of social space, especially through social networking, which provides additional opportunities to meet people and have fun.[49] Adults may perceive the online and offline worlds as being quite different, but for many children and young people who are building social networks through making friends in both worlds, the distinction has little significance. In this sense, the online and offline worlds are merged.

Clear boundaries used in the physical world to keep different aspects or contexts of life separate do not necessarily exist or operate in the same way online.[50] SNS apply the concept of 'friendship' to anyone listed on one's profile. On the one hand, boundaries may seem initially less important, as people met are not physically present. Studies from several parts of the world suggest that young people often feel safer sharing highly sensitive personal information or engaging in sexualized behaviour online than they do offline.[51] On the other hand, online forums – whether chatrooms, blogs, online gaming or social networking sites – deconstruct traditional boundaries of privacy. Children engaged in 'chat' or 'conversation' in the private space of their own bedrooms can expose themselves, wittingly or unwittingly, to an unknown worldwide audience, potentially increasing the risk of harm. Information posted online creates a historical record of the child, diminishing control over who has access to personal data and sometimes trapping children who may find out too late that they cannot retrieve what they have put online. Warning signs that can serve to protect children in the physical world are largely absent online. In the physical world, a range of filters exist, such as body language or warning cues from a potential 'friend' as well as their degree of geographical proximity. The many mechanisms that have been developed to safeguard children in the offline environment do not yet exist in the online world.

Understanding risk, vulnerability and harm

There are major differences between risk and harm, and policymakers and parents need to keep these distinctions clear. Certain types of activity may involve risks that do not necessarily result in harm to children and young people. Swimming, riding a bicycle or joining an SNS may confer benefits but also involve risks and, under certain circumstances, might expose a child to harm. Most significantly, as regards the Internet, there is no easy line that can be drawn between activities leading to benefits and those leading to risks.[52]

Concern is often expressed among adults about the risks associated with posting information and images online. Hence, much research starts from the premise that posting information is in itself risk-taking behaviour. Young people are indeed posting information that adults may find disturbing. A wealth of evidence from across the globe shows that many young people, particularly in the age range of 12 to 16 years, are placing highly personal information online. In Brazil, for example, surveys indicate that 46 per cent of children and adolescents consider it normal to regularly publish personal photos online, while a study in Bahrain indicates that children commonly place personal information online, with little understanding of the concept of privacy.[53] In addition, significant numbers of teenagers are uploading visual representations of themselves that are sexual in tone.[54] This is sometimes in response to grooming that involves encouragement to place such images online, which may be followed by blackmail or threats of exposure to coerce teenagers to upload increasing numbers of explicit images. But in other cases, the initial placement is unsolicited, and may encourage and attract potentially abusive predators.

Another increasingly common behaviour by teenagers is 'sexting' (sharing of sexualized images or text via mobile phones).[55] These images and text are often shared between partners in a relationship or with potential partners, but sometimes end up being shared with much wider audiences.[56] It is thought unlikely that young teenagers have an adequate

understanding of the implications of these behaviours and the potential risks they entail.

There is, however, considerable debate about the issue of placing information online. It can be argued that posting personal information online is becoming normal behaviour.[57] Basically, if a young person is not posting personal information, their peers will not consider the page lively or interesting. They may even regard them as being a little odd or stand-offish. Putting information online is part of their cultural context and therefore commonplace, and the majority of young people do not appear to be harmed by it.[58] Research from the United States, for example, has found that, in general, there is little evidence that the everyday placement of personal information online, including images, leads to personal victimization of children. It is online interaction and engaging in many different types of risky behaviours online rather than posting information that creates the environment that enables sex abuse and grooming to unfold.[59] Not only is it unrealistic to change normative behaviours, but the evidence suggests that it is probably not useful or necessary to try to do so.

There is insufficient evidence to provide an unambiguous indication of whether the risks associated with online activities are the same or have the same implications for children across different regions of the world. In many African and Asian countries, for example, widespread poverty and weak state structures undermine children's social and legal protection and therefore may contribute to increased vulnerability.[60] Findings about other particular characteristics that may make children vulnerable to sexual abuse and exploitation online are contradictory. Research from South Africa and the United States suggests that children with low self-esteem or children experiencing depression, negative life events, or offline abuse or victimization are at a particular risk of being groomed online.[61] Findings from studies in the United Kingdom report no obvious pattern of particular vulnerability in the offline world.[62] Research in Brazil found an important link between social factors and economic conditions. Girls from favelas (informal settlements) are exposed to earlier sexualization and are more likely to socialize with older age groups who they perceive as raising their social status. They identified using the Internet as an instrument to enable them to visit sexually oriented sites and meet boys. Middle-class Brazilian girls, on the other hand, who appear to have more adult monitoring and guidance than those from the favelas, reported using the Internet mainly for educational purposes.[63]

Furthermore, in the lower-income countries, children are less likely to use the Internet from home and, even if they are at home, their parents are likely to have far less understanding of the nature and risks associated with the online environment, thereby reducing the opportunities for parental protection and support. Children accessing the Internet through cybercafes in Brazil, India, Nepal and the Philippines identify these places as particularly hazardous, potentially exposing them to adults who use pornography, to pornographic material, to solicitation or to drugs. Coupled with this is the likelihood that in countries where children are more reliant on Internet access through cybercafes, there is less regulation, less opportunity for reporting and, in many cases, little overall investment in building a protective environment.[64] However, it is clear that while Internet usage in the privacy of one's home may appear less hazardous, it is more accurate to state that while certain dangers are reduced or are not present in the home, others depend on the types of activities children are engaged in online.

Some of the available research disaggregates data on the basis of gender, which provides useful information on the differences and similarities related to Internet risk, vulnerability and harm experienced by boys and girls. But there are many groups about whom no evidence exists. For example, ICT may offer numerous potential benefits to many children with disabilities, such as communication for those unable to move about freely in the physical world, greater access to the written word for children with visual impairment and capacity to communicate freely for children with hearing impairment. However, it is not known whether children with disabilities might be drawn towards greater dependency on online relationships and whether they are consequently more vulnerable, whether among this group the desire to construct alternative identities is greater than among other children, or whether they are at greater risk of targeted grooming. Similarly, LGBT young people, particularly those living in environments in which they are unable to express their sexuality openly, may gain hugely by being able to use the Internet to build friendships with persons sharing their sexual orientation. Conversely, however, greater dependence on the Internet may render them more exposed to risk of abuse. There is some evidence that LGBT young people are particularly vulnerable

to cyberbullying.[65] Given the importance of supportive parental relationships as a protective factor, research to gain a better understanding about the risks migrant or other children separated from their families face in the online environment would also be useful.

In terms of young people's own awareness of online risk, surveys from Brazil and countries in Europe suggest that many children are aware of basic hazards, but that most do not perceive themselves as vulnerable. Children think that 'others' (for example, younger and inexperienced children) are at risk, rather than themselves.[66] Many children and young people who use SNS are aware of the challenges concerning security of information, have felt pressure to post personal information when they did not feel comfortable doing so, and have some anxiety that they are visible to many people they do not know. However, a national survey indicates that in the United Kingdom, this has little impact on their behaviour unless a problem has affected them personally or has been thought to be serious.[67]

Overall, there are widely differing perceptions among children and young people of the dangers associated with the Internet. While there is little comparative research available to provide clear evidence on how different perceptions arise, these seem to relate to availability of information, location of use and awareness of safe reporting mechanisms.

Parents or peers: Who do children turn to for support?

Research from around the world indicates that children and young people have far greater confidence about their ability to remain safe online than their parents.[68] Broadly, however, children appear less confident about keeping safe in countries where Internet safety information is not widely available. European research from 2009 found that parents are less likely to worry about children's online safety if they themselves go online. Once they better understand the online environment, parents gain a more informed perspective of the risks involved.[69]

In terms of protection from harm, the evidence consistently indicates that children often do not see parents as an automatic first port of call when they experience abuse. The level of involvement of parents varies, however, according to several factors, including country, age and level of parental Internet use.[70] Explanations of why children do not look to their parents for protection from online harm include children's beliefs that their parents do not understand the world in which the abuse takes place, their fear of having mobile phones taken away or Internet access restricted, threats by the abuser, or shame and humiliation.[71] Whatever parents may wish, some adolescents do not want adults interfering. Adolescence tends to be a developmental stage that involves exploratory behaviour and pulling away, to a degree, from parents. They may thus perceive parental presence and involvement in their social space and online interactions as interference.

Nevertheless, a growing body of evidence from the industrialized world identifies the strongest protective factor for children to be actively engaged parents who share Internet experiences with their children and are willing to talk about the issues involved.[72] Respect for, and interest in, children's engagement with the online environment are likely to be more effective than restrictive or punitive controls. Furthermore, research suggests that many children and young people would like parents to be more involved. For many children, exclusion of parents seems not to inevitably derive from reluctance for their support, but rather from the child's perception of limited parental capacity to effectively provide support.[73]

Parental capacity to protect children is also increasingly limited by the fact that many of the activities previously done via computers based in fixed locations are now being utilized on mobile phones with Internet connectivity. When children have access to such phones, as an increasing number do, parents are less able to monitor their children's activities, introduce filtering or blocking mechanisms, or control the degree of access to the Internet. This changing pattern of usage presents fundamentally different challenges that need to be acknowledged in the introduction of protective or preventive strategies.

A consistent message emerging from the research is that children and young people see themselves as 'protectors' of other children. Children tend to first turn to each other when in need of help. Young people demonstrate high levels of concern and awareness of risks for young siblings, friends and others they perceive as more vulnerable than themselves.[74] This suggests a potential role for children as peer educators, mentors and advisers. In the context

of the sociology of actual Internet use, listening to children and supporting them to be the front line in taking care of themselves and each other is likely to be one of the keys to reducing both risk and harm.

Children's use of the Internet, and their behaviour and vulnerabilities within the online environment, differ according to their age. Recognition is needed of the evolving capacities of children, with protection strategies that are appropriate to their age and level of understanding. As yet, there is relatively little known about younger children's online experience, although there is a growing body of evidence that shows that, in industrialized countries, many children under eight years old are now accessing the Internet, either through computers or mobile phones. More research is needed on usage by younger children and how to respond most effectively to protect children of different ages and capabilities.

The challenge for those who place an emphasis on protection by adults is whether in reality such a model can be effective in the context of the fast-changing online world, especially in cases where parents lack understanding of the Internet and the role it plays in their children's lives. Conversely, the challenge for models that place trust in children is to ensure that this assurance is well placed and that children are socially and technically empowered and supported to be able to look after themselves and others. The reality is that both approaches must reinforce each other.

Programmes designed to support children and young people to make informed choices, based on a genuine awareness of the nature of risks involved, need to accommodate an understanding of adolescent sexuality, role of the peer group, adolescent cultural expectations, and assumptions about risk from the perspectives of children and young people. Risk-reduction messages, for example, need to place emphasis on the problems that can arise from interacting with people met online, rather than trying to impart prevention messages that sound sensible to adults but do not relate to normal use or the nature of risk as perceived by young people.[75] An example of such messages might be "don't post personal information". Online risks can be minimized provided there are external mechanisms to regulate the environment, strong and supportive parental relationships, together with knowledge, skills and awareness that enable the child or young person to navigate the online environment effectively.

The responsibility to protect children in the online environment should not be borne only by parents and children. Policymakers, professionals, such as teachers and social workers, law enforcement agencies and the private sector all have a role in creating a safe external environment that allows children and young people to benefit from the use of modern technologies without experiencing harm.

PART TWO

BUILDING A PROTECTIVE ENVIRONMENT

There is much to be done in all parts of the world, industrialized, middle- and low-income countries. A comprehensive protection response entails action involving a diversity of governmental and non-governmental actors across a range of spheres. This includes putting the 'architecture' in place – a legislative framework to define criminal activity, the capacity to deter potential abusers and prosecute offenders, and proactive measures to restrict and inhibit access to child abuse images by actual and potential offenders. It also includes strengthening joint work and intersectoral collaboration between the justice and social welfare sectors. It requires improving awareness of child protection services, educating other professionals who work with children, such as teachers, on the nature of risk and harm in the merged online/offline worlds, and implementing measures to support children to stay safe. It involves promoting strategies to empower children to avoid harm. Investment in welfare measures is required to address the needs of children who have been harmed through sexual exploitation and abuse via the Internet and to build the capacity of professionals who work with them.

Given its central role in designing and driving the Internet, the private sector must recognize that contributing to the wider social goal of making the Internet safer for children and young people is intrinsic to expanding access and innovating content. As Livingstone and Haddon have pointed out, as use of the Internet becomes more personalized, the role of parents or teachers becomes more difficult, which places even greater responsibility on industry to manage the risks that children may encounter.[76] Failure to do this will expose the industry to risk of governmental or regional regulation that has a negative impact on the freedoms embodied in the Internet as it is today.

A broad response requires working directly with young people in the design and implementation of information and protection strategies. Children and young people need information about risks and how to avoid them, and the mechanisms and pathways to follow if they find themselves in situations they judge to be dubious. They need skills to make informed choices in their cyberspace activities and to provide each other with support. This is increasingly important as Internet usage becomes more private (i.e. takes place in children's private spaces, such as bedrooms, in much of the industrialized world) and more mobile. Child protection mechanisms must be transparent, accessible and enforceable. If children are to use them, they must feel safe and be perceived as effective. The active engagement of children in online protection strategies provides an essential source of experience and expertise.

Building parents' abilities to support their children is also a vital component for online safety. This is not to place the responsibility for protection on children and parents alone, but to recognize reality. The nature of the social space provided by the Internet and the fact that young people are pacemakers in its exploration and use mean that they must be at the forefront in solutions to reducing risks, and parents are in one of the best positions to support them. Parents need to be made aware of the nature of risks and encouraged to improve their understanding of young people's online activities.

In the industrialized world – country by country, to a greater or lesser degree – some of these

elements are coming together. However, greater levels of coordination are required in the work that is being undertaken. In many low- and middle-income countries, awareness of the nature of risk and the capacities to reduce or respond to it are nascent at best. By its very nature, abuse on the Internet has no borders; coordinated international action by justice and welfare sectors is therefore essential.

International instruments and commitments

Like a number of other child protection issues, online abuse and exploitation of children is at the intersection of two sets of international standards. Taken together, they provide a framework to address the phenomenon and inform the creation of a protective environment for children. On the one hand, some international instruments focus on abuse and exploitation as a child rights violation, in the broader context of the promotion and protection of children's rights and their interdependence and indivisibility. On the other hand, several international instruments aim to address various forms of transnational crime, and while taking into account the human rights of persons affected, tend to concentrate on response and prosecution.

In this context, the five main international instruments are:

- Convention on the Rights of the Child (1989)
- Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (OPSC, 2000)
- Protocol to Prevent, Suppress and Punish Trafficking against Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime ('Palermo Protocol', 2000)
- Council of Europe Convention on Cybercrime (2001)
- Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (2007).

Not only do these instruments provide guidance on addressing and responding to sexual exploitation and abuse of children in the online environment, they also establish a set of legally binding obligations for States Parties to take specific measures in this respect. Together, they elaborate a comprehensive framework of child rights, including definitions of offences and provisions that require punishment for criminalized behaviour, and allow for more effective prosecution of perpetrators. The Convention on the Rights of the Child has a particular significance because it places protection alongside other rights particularly relevant to the benefits the Internet brings – freedom of expression, freedom to seek information and freedom of association. The OPSC and the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse also serve as comprehensive examples of legal mechanisms that require governments to implement and ensure provision of services to assist child victims and their families.

Although regional instruments have specific application only within the region in which they are developed, they establish standards or benchmarks for other countries to adopt and comply with, and in some instances allow for ratification by States from outside the region. While under international law States have the primary responsibility to ensure respect, promotion and protection of children's rights, the Convention on the Rights of the Child and additional instruments have recognized that other actors – such as parents, civil society, private sector service providers and businesses – also have a critical responsibility in this regard.

Since the 1990s, the United Nations and related bodies, as well as various regional bodies, have made additional commitments and have adopted guidelines and codes of conduct designed to strengthen child protection mechanisms. Progress was accelerated with the appointment in 1990 by the Commission on Human Rights, of the Special Rapporteur on the sale of children, child prostitution and child pornography; the Commission's adoption in 1992 of a Programme of Action; and subsequently by the three global congresses against Sexual Exploitation of Children (Stockholm 1996; Yokohama 2001; Rio de Janeiro 2008), which reaffirmed the human rights-based goal of universal protection of children from all forms of sexual exploitation.[77]

The World Congress III in 2008 led to the 'Rio Declaration', which calls on States to undertake specific and targeted actions to prevent and stop child abuse images and use of the Internet

and new technologies for the grooming of children into online and offline abuse, and for the production and dissemination of child abuse images and other materials.[78] The earlier 'UN Study on Violence against Children', reported to the United Nations General Assembly in 2006, also recognized the need for governments to "strengthen efforts to combat the use of information technologies…in the sexual exploitation of children and other forms of violence."[79]

However, despite the increased focus on sexual exploitation and abuse of children at the international level and the development of these new global and regional human rights instruments, there continues to be a lack of systematic implementation of the necessary legislation and subsequent action at the national level. For example, in its ongoing review of legislation related to child pornography, the International Centre for Missing & Exploited Children has indicated that, as of 2010, only 45 of the 196 countries reviewed had legislation sufficient to combat child abuse image offences, and 89 had no legislation at all that specifically addressed child pornography. Of the countries that do have legislation in place, 52 do not define child pornography in their national legislation; 18 do not provide for computer-facilitated offences; and 33 do not criminalize possession of child pornography, regardless of the intent to distribute.[80]

At regional level, the European Union has recognized the need for collective action in combating the sexual abuse and exploitation of children, arguing that while national legislation covers some of these issues, it does not address sexual abuse and exploitation of children through ICT nor is strong or consistent enough to provide an effective response and protection to child victims.[81]

Accordingly, in November 2011, the EU adopted the Directive of the European Parliament and the Council on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA. Among other actions, the Directive will criminalize forms of child sexual abuse and exploitation not currently covered by EU legislation, such as grooming, online pornographic performances and viewing child pornography without downloading files; establish lower thresholds for applying maximum penalties; ensure that offenders who are EU nationals face prosecution for crimes committed outside the EU; provide child victims of the offences covered with assistance, support and protection, including for claiming compensation; share data relating to the criminal convictions of sex offenders between relevant authorities in member States; and introduce mandated removal and optional blocking of websites containing child abuse material.[82]

The EU was an early champion of self-regulation as a means of keeping young people safe online. In February 2007, leading mobile operators and content providers across the EU signed the European Framework for safer mobile use by younger children and teenagers. As of June 2010, codes of conduct were in place in 25 EU member States, while under development in the remaining 2. The Framework commits signatories to principles and measures, including access control for adult content, awareness-raising campaigns for parents and children, and the classification of commercial content according to national standards of decency and appropriateness. A June 2010 implementation report found that it had been effective, with 83 mobile operators, serving 96 per cent of EU mobile customers, implementing the Framework through the codes of conduct.[83]

In February 2009, two years after the adoption of the code on the safer use of mobile phones, the European Commission facilitated the production of a document entitled *Safer Social Networking Principles for the EU*, which was launched with 21 signatories from all of the largest SNS operational across the 27 member States. Privacy settings are a major focus of the principles, but there are also important provisions in relation to education and awareness-raising activities and reporting abuse. A second assessment of the social networking principles was published in May 2011. Here the findings were more mixed; of the 14 SNS that responded to the survey, only 3 received high ratings in relation to explicit information regarding the characteristics (e.g. age-appropriateness, availability, user-friendliness, etc.) of privacy settings.[84]

In June 2011, the European Commission held its first Digital Agenda Assembly. This included a specific workshop entitled 'Every European Child Safe Online' where Digital Europe, the trade association for a broad spectrum of high-tech companies, presented a draft proposal to develop a new high-level framework of rights and responsibilities. Work on the draft is expected to be completed by early 2012.

Although there are at present no inter-American protocols or instruments specific to the

protection of children in the online/offline environment, relevant regional materials do exist. The 'Memorandum of Montevideo', developed in July 2009 by a group of regional experts, provides a framework for protecting children's personal information in cyberspace.[85] Designed to guide legislators, judges, policymakers and law enforcement officers on how to protect children's personal data online, the memorandum lists recommendations on prevention and education, legal frameworks, law enforcement and public policy.[86] Although the memorandum is not binding on any Latin American state, it acts as an important framework for states seeking to protect children's personal information online. Within Africa, Asia and the Middle East, regional coordination does exist, but it is largely ad hoc.

Challenges for law enforcement and child protection

Legislation and political commitments, while of fundamental importance, cannot achieve change without mechanisms in place to implement and enforce them, and services to provide support to victims. Law enforcement agencies are charged with the responsibility of ensuring that laws are applied consistently and effectively and offenders prosecuted and held to account. They therefore have a vital role in challenging sexual exploitation and abuse of children in the online/offline merged environment. Social welfare agencies have a responsibility to promote and protect the best interests of children who have experienced abuse. However, these two agendas may sometimes come into conflict. The challenge is to explore approaches that are both effective at bringing about successful prosecutions while also ensuring that the interests of the individual children concerned remain the paramount consideration.

The online environment of the 21st century has transformed criminality in a number of ways: as an advanced vehicle for communications, it has created a transnational environment that provides new opportunities for harmful activities, and the virtual nature of the online environment means criminal activity can sometimes fall outside the jurisdiction of the criminal justice process.[87] Crime prevention may no longer be only about surveillance and investigation within the immediate community but instead may cross local, national and international boundaries. It may not be easy to assign a jurisdiction to a crime committed in the virtual environment. Moreover, particular crimes might also involve many victims from different countries, thus complicating legal and child protection processes even further. Crimes of online sexual abuse and exploitation may involve offenders who perpetrate them in locations thousands of miles away from the child victims. This poses serious challenges and requires greater collaboration among the police forces in different countries, spanning very different jurisdictional protocols, social and cultural environments, political expectations, and levels of capacity, technical expertise and resources.[88]

Establishing that a crime of online sexual exploitation or abuse of a child has occurred is often not a straightforward process. A unique characteristic of the online environment is that physical contact between a child and an offender does not need to occur for a crime to have been committed. The challenges for law enforcement agencies are particularly great when the law does not provide clear definitions of criminal activity. For example, to establish that a crime has been committed is it sufficient to establish 'intent' to lure a child even if no actual physical contact has been made; what evidence of 'intent' is required; what constitutes a 'pornographic' image of a child? In some jurisdictions, for example in Canada and the United Kingdom, both simulated and real images of children engaged in sexual behaviour are criminalized.

Children who are the subject of child abuse images or those groomed for sexual exploitation may experience feelings of shame and complicity. Therefore, many victims of Internet crime do not disclose their experiences until the pictures or images are discovered, most typically by law enforcement agencies during an investigation. However, even here matters can be complicated. There have been recorded cases where even though law enforcement officers were in possession of images of a child being abused, the child being victimized has gone into denial and refused to acknowledge that they were featured.[89]

Most sexual abuse of children goes undisclosed. When that abuse takes place online, the level of disclosure is even lower.[90] Some children who have been abused perceive the persons they have formed a relationship with online as their boyfriends or girlfriends, and they are emotionally dependent upon them.

Some children who are vulnerable to grooming may be isolated and lacking in social support, and are thus less likely to report victimization to law enforcement agencies and others. Furthermore, many children do not realize that they have been victims of a crime because innocent images of children may be digitally transformed into pornographic material and distributed across the Internet without the victim's knowledge.[91]

The disclosure of abuse entails several challenges that are often underestimated and misunderstood. Children need acknowledgement of their feelings and fears in order to cope with this experience. It is not unusual for children to retract their allegations due to fears of repercussions on them, their family, others who are important in their lives and the perpetrator of the abuse. Children are not only affected by the abuse itself, but may also be further traumatized by the disclosure or its consequences.[92]

The process of identifying children who appear in child abuse images in order to protect them and offer appropriate psychosocial support can be difficult. Images on the Internet can circulate for many years, so a picture of a 5-year-old girl, for example, may still be online 20 years later. To help identify victims, INTERPOL (the International Criminal Police Organization) and some national law enforcement agencies have produced databases of child abuse images. By applying sophisticated image analysis software, the police can assess whether an image of a child contained within, for example, a collection that has just been seized, is identical to ones that have already been discovered by law enforcement agencies, and included in a database of known images. Some of the software can also help identify children who have been abused over long periods of time, whose physical appearance may have changed dramatically as they grew older. This is important both for the development of a comprehensive case against an alleged perpetrator and for determining the duration and nature of the abuse a child has suffered in order to support recovery.

Databases of victim photographs are valuable resources. They can save a great deal of police time and reduce the need for officers to look at the images directly. This latter aspect is particularly important. Until relatively recently, police work often necessitated repeated viewings of images. However, new technology has been developed that enables photographic images to be reduced to a digital code, known as a 'hash', which can then be used to track, trace and compare images, without a police officer needing to view the actual image.[93] The United Nations Special Rapporteur on the sale of children, child prostitution and child pornography has pointed to the need for explicit ethical policies that clarify how the images are used, who has access to them, in what circumstances, and the rights of victims to information about where and how the images are held.[94] Police units and hotlines that handle child abuse images will typically have in place protocols that govern the amount of time and the locations for viewing and storage of images. The harrowing nature of the images may pose a challenge for those who work with them. It is not uncommon to find that counselling services are made available to police officers and staff who work in hotlines where viewing abuse images is an unavoidable part of the job.

The Internet is commonly perceived to offer users, including potential offenders, anonymity, enabling them to construct identities and determine when, how and to what extent personal information is communicated to others in the online environment.[95] By so doing, their personal identity or personally identifiable information remains private. This presumed anonymity creates a sense of security and secrecy for both offenders and potential victims.[96] Traditionally, in an offline context, in order to find their victims child sex offenders needed to stalk playgrounds, social clubs and other public places where children tended to gather. Today, the high level of social interaction by children online provides offenders with a new environment to target children, and the risks that they previously faced when making face-to-face contact may appear to them, erroneously, to have been eliminated.

Investigations into online criminal activity are complex and time-consuming. They often involve coordination across jurisdictions and concern a huge network of offenders. There are a number of constraints to effectively carrying out such investigations. The first is limited specialist expertise. Tackling online/offline child sexual abuse and exploitation requires combined expertise in policing, computer and Internet technology and child protection. Specialist units are largely absent in many middle- and low-income countries, meaning that staff are unlikely to have the necessary training to investigate online crime. Even where staff do possess the requisite skills, the technology to investigate such crimes may not be available. Consequently, many law enforcement officers are at a disadvantage in

detecting, investigating and prosecuting online-related crime.[97]

Another challenge is the lack of multi-agency collaboration and coordination. Law enforcement departments may not always view online sexual exploitation as a protection issue. Rather, in many countries, online/offline sexual exploitation is categorized as 'cybercrime'. E-crime or cybercrime police units are often primarily focused on fraud and organized crime and may therefore have little or no expertise, or professional interest, in child protection. Whereas commercial child abuse websites may legitimately be classified as organized crime or be investigated by police officers more accustomed to dealing with fraud or terrorism, much of the exchange of sexual abuse images and grooming does not fall under this umbrella. Police need to deliver a child-centred response, which rarely happens when they investigate online abuse and exploitation of children on their own. The integration of child protection specialists into an investigation, a practice recommended by the Child Exploitation and Online Protection Centre (CEOP) in the United Kingdom, ensures that the young person is adequately safeguarded and their welfare is taken into account at each stage of the investigation.[98]

There is limited evidence available on how social welfare professionals are responding to the new challenges of child protection in the online/offline environment. Two recent reports point to a lack of knowledge and awareness among social workers of the risks of Internet abuse. Although both are from northern Europe (Germany and Norway), the pattern they identify is likely to be replicated elsewhere.[99] The studies suggest that, in general, professionals who come into contact with children – schoolteachers, nursery and school nurses, health personnel, police officers, social workers and counsellors/psychotherapists – are not sufficiently aware of the risks of abuse via new technologies. If, for example, they were concerned about changes in a 13-year-old's behaviour, they might not consider that the child could be the victim of abusive behaviour online, and therefore would not ask the child about his or her online life. Furthermore, these professionals are not always prepared or able to hear what children want to tell them. The causes identified include lack of professional confidence, inadequate training, work pressure, emotional barriers, their own values, attitudes and beliefs, insufficient knowledge of the issues and lack of support. Bearing in mind how increasingly central ICT is to children across the world, this lack of awareness means that professionals are failing to identify and investigate an increasingly important context for abuse.[100]

To gain an overview of available rehabilitation and therapeutic services for children who have been abused or exploited online, an ad hoc survey of professionals and researchers with expertise in the field was conducted as part of this study.[101] Responses were received from 10 of the 20 countries that were invited to participate – Australia, Bahrain, Denmark, Germany, Iceland, India, Latvia, the Russian Federation, South Africa and the United Kingdom – and they produced the following findings:

- In some countries, there is separate and distinct guidance for the police and social workers; in others there is guidance only for the police. In some countries, the existing guidance is not adhered to and is out-of-date.
- Staff in centres that offer recovery services to children who have experienced trauma report they do not feel confident in working with such cases.
- Six countries were able to describe examples of national/regional police and social workers working together. These included specific investigations that had been carried out and ongoing service delivery, such as hotlines.
- Nine of the 10 countries consulted do not have national systems for recording the numbers and nature of Internet-mediated crimes against children. Within some countries, there are pockets of information from sources, such as helplines, CEOP and ad hoc recovery services. Iceland, however, was the exception. It has one central point-of-call through which child protection referrals are channelled. Known as Kinder House (Children's House), it offers a universal service to all children throughout the country who have been victimized, and runs a multidisciplinary model working in partnership with police, social workers, lawyers and counsellors.
- Four of the respondents stated that there were no examples of their country working collaboratively on international investigations; one additional respondent did not know of any, while the remaining five described complex international operations that have lasted several months and involved a number of countries, which have resulted

in children being safeguarded and the perpetrators of abuse being convicted.

- Bahrain, which has little in place regarding a strategic response to Internet-related crimes against children, reported that it had conducted a *State of the Nation Review of Internet Safety* in 2010. In addition to providing a comprehensive analysis of Internet safety issues among adults and children, it establishes recommendations for child Internet safety.

While this survey was limited in scope and conducted specifically for the purpose of this project, these findings reveal a mixed pattern of provision. Some good practice does exist, but there is a need for more systematic and coordinated processes across government and involving all relevant agencies, if effective protection of children is to be achieved.

A framework for response

Recognizing the major benefits the Internet and associated technologies can bring, the huge potential to transform lives and the way they have become integral to modern society and are now an intrinsic part of young people's social landscape, this report proposes a strategic framework for protection that addresses four key objectives:

1. Empowering children and enhancing resilience to harm

In much of the reporting of Internet crimes by the media, there is a tendency to portray children and young people, particularly girls, as actual or potential victims with little agency. With regard to online child abuse images, which generally involve children younger than 10, their consent or capabilities usually have little bearing on whether or not they have come into harm's way. However, studies from across the globe indicate that for online grooming or cyberbullying, child agency is critical.

Specifically in relation to grooming, young people's experimentation, exploration and interest in defining themselves socially and sexually are all risk factors. Conversely, young people's exploratory orientation enables them to access the many benefits of the Internet in terms of education, culture and creativity. Hence, preventive and protective responses must take into account the extent to which children's participation in online communication potentially engages them in risk-taking behaviour but also plays an important role in their identity construction, self-efficacy and social network production in a social space that young people have made their own.

Active participation by children and young people in developing and implementing protective measures will lead to strategies that make sense to them and are therefore more likely to be effective. Ensuring that they have the best possible information about the nature of risks associated with online activities, empowering them to take the necessary actions to prevent exposure to harm, and providing them with necessary support from key adults in their lives are all important. Children and young people need to know where to go for help, recognizing that they, themselves, are a key source of much of that help. They need opportunities and means to report unacceptable activity or behaviour, counselling when needed, and confidence not only that action will be taken when they are harmed or abused, but that they will be respected as active agents. This will involve:

- *Providing information to children that enables them to make informed choices, avoid risks, and find and offer help when needed.* Many countries have developed innovative materials to communicate with children that can be adapted to different country contexts. SaferNet Brasil, for example, has created an educational kit on Internet safety designed for educators with the aim of improving their students' online safety.[102] In the Bolivarian Republic of Venezuela, the children's group Manos por la Niñez e Adolecencia (Hands for Children and Adolescents) promotes Internet safety for children, adolescents, adults and Internet cafe owners.

- *Introducing effective reporting mechanisms, such as hotlines, report abuse functions, and online supports to pre-empt abusive situations.* In some social networking sites, an icon on the home page allows children who are worried about the behaviour of someone communicating with them can, with one click, share their concerns and then be linked to a law enforcement agency.

- *Strengthening parental capacities to protect children* through programmes that inform parents about the benefits and risks associated with ICT, strategies that

children and young people can adopt to keep safe, potential sources of help, and the importance of dialogue and engagement with their children.

- *Building capacity among professionals who work with children to alert them to the risks children face and teach them how to recognize warning signs and symptoms.* In Thailand, for example, a digital literacy initiative on safe Internet usage resulted in a training module which has been used to train some 300 teachers. Those teachers subsequently delivered safety messages to more than 70,000 children.[103]

- *Involving children as campaigners and advocates, and utilizing their unique insights and experiences to inform the development of more effective protection.* In Benin, the Gambia, Kenya, Mozambique, Nigeria, South Africa and Togo, with ECPAT support, young people have created public awareness campaigns on the risks associated with the online environment and the responsibilities of governments and ICT providers to ensure better protection of children online.[104]

- *Tackling cyberbullying through the development of initiatives that promote a commitment to zero tolerance of violence and abuse in schools*, including cyberspace, and that create educational measures based on principles of acceptance, respect and decency among students.[105] In Croatia, for example, a national campaign to confront cyberbullying led to significant changes in schools, including the reduction of violence.

2. Removing impunity for abusers

As long as abusers are confident that they can get away with exploiting or abusing children without the risk of prosecution or social condemnation, they will continue to do so. It is therefore essential to remove impunity for those who continue to do so in the merged online/offline environment.

Sexual abuse and exploitation of children online is a global problem that can only be addressed effectively through coordinated action at all levels: national, regional and global. Without this commitment, perpetrators of child abuse may choose to concentrate their efforts in countries that offer the least protection to children and where exploitation is, from their perspective, easier to carry out and less likely to be detected and prosecuted. Building a common approach across jurisdictions is important, as it allows for consistency in criminalization and punishment, raises public awareness of the problem, increases services available to assist affected children, and improves overall law enforcement efforts at the national and international levels.[106]

Given the huge differences in existing legal frameworks in jurisdictions across the world, safeguarding children from online abuse and prosecuting abusers presents a daunting challenge. Drafting legislation to protect children in the merged online/offline environment is complex. Establishing a coherent global approach intensifies the difficulty of that task significantly. Building an environment that challenges the 'cost benefits' to abusers and removes their impunity requires a holistic approach. Such an approach must seek to secure the indivisible nature of children's human rights, and must be global, implementing the relevant international standards and promoting collaboration and communication among governments.

The following key approaches are proposed as fundamental building blocks in establishing the legislation and law enforcement framework required to remove impunity for abusers:

- Introduction of effective national legislation, including clear definitions of a child, sexual consent, and what constitutes child pornography or child abuse images; the criminalization of the sexual exploitation of children by adults, including possessing, downloading or creating child abuse images, grooming, sexual abuse without contact and attempt crimes; effective sanctions and penalties; and measures to address the challenges of jurisdiction and extradition.

- Adoption of a broad range of law enforcement strategies, including close collaboration with social welfare and child protection agencies, covert operations and victim identification. Social workers, teachers and psychologists can provide invaluable guidance to ensure the use of appropriate interrogation and interview techniques, and can help police maintain a clear focus on the protection of victims during the prosecution of offenders. Some countries, including Australia, Canada, New Zealand, the United Kingdom and the United States, which work together as part of the Virtual

Global Taskforce, have introduced specialist units that focus on the prosecution of online sexual exploitation and abuse of children, enabling different professionals to collaborate on cases.

- Cooperation with Internet service providers (ISPs), the online payments industry and other private sector stakeholders to track child sex abusers and to close down channels to this type of crime. Examples include: the Financial Coalition against Child Pornography, set up by the National Center for Missing & Exploited Children in the United States and supported by banks and other institutions; and the European Financial Coalition against Commercial Sexual Exploitation of Children Online, which was initially led by CEOP and supported by MasterCard and Visa, among others. In 2009, the Financial Coalition in the United States established an Asian initiative involving banks and financial institutions based in Singapore. Microsoft has also partnered with law enforcement agencies and ISPs in various countries to develop initiatives to stop child sexual exploitation over the Internet.

- Consideration of mandatory reporting by professionals who work with children on suspected abuse, bearing in mind that effective reporting is dependent on the quality of services available to respond to reports.[107] Mandatory reporting could be extended to include others who may discover evidence of child sex abuse as a consequence of their profession (for example, ICT professionals, photo developers and computer servicing companies).[108]

- Collaboration among law enforcement agencies at the international level and the development of tools that help gather evidence in criminal cases and facilitate data exchange among police forces across countries. INTERPOL, for example, coordinates large-scale investigations that involve multiple member countries and utilize an effective law enforcement tool known as the 'Green Notice'. The tool alerts the international law enforcement community to offenders who are likely to repeat the same crimes in other countries.[109]

- Assurance that children involved in online sexual offences will not be held criminally liable. Children should be acknowledged as victims, regardless of whether they are a compliant victim or a non-cooperative witness. Where children under 18 are engaged in sexual abuse or harassment online and the child's behaviour was deemed to be illegal, the response of States should be through the juvenile justice system in collaboration with the child protection system, rather than the criminal justice system, in line with international standards.[110]

3. Reducing availability and access to harm

While the primary goal is the elimination of online/offline sexual exploitation and abuse of children, the reality is that many millions of child abuse images continue to be available on the Internet and are likely to remain there for the foreseeable future. Strategies are needed to reduce the numbers of images being created, stored and circulated, as well as to limit access for both potential abusers and the children who may encounter harmful sites while online. The continued presence of child abuse images encourages further exploitation of children, leads to increased numbers of abusers, and results in children being exposed to repeated and indefinite abuse. The best interests of children must be ensured by making the greatest possible efforts to ensure that their images are quickly removed from further circulation, that access to commercial sites is blocked, and that mechanisms are introduced to limit availability and access.

Some children will continue to behave in risky ways regardless of the information provided to them, through their spirit of exploration, lack of awareness of the implications of their actions both socially and in terms of the nature and consequences of technology, misplaced confidence that they are in control, and assumptions that it is others, not themselves, who are at risk.

As stated earlier in this report, the ICT industry has an important set of responsibilities to discharge in relation to reducing risk. While leadership by committed companies is essential, so too is collective action. To stem the availability of abuse images and reduce harm, close collaboration is required by governments with private sector actors, including ISPs, social networking sites, Internet cafe owners and site-hosting services. Joint efforts should include:

- Developing codes of conduct and systems of self-regulation. These offer a mechanism

through which businesses can express and meet human rights standards by adopting voluntary, non-binding best practices as a guide for management and employees. Drafting codes of conduct poses challenges, as companies may consider profits, public relations and human rights as mutually antagonistic. The experience of the United Kingdom suggests that codes of conduct that are not linked to demonstrably independent and effective means of monitoring performance will fail to inspire public confidence.[111] A conflict of interest may arise if multinational companies monitor themselves or are monitored by their subcontractors. Without independent third-party monitoring there may be little real incentive for a business entity to observe the terms outlined in the code.

- At the local level, promoting codes of conduct in Internet cafes to encourage owners to introduce measures that will prevent children who use their establishments from being exposed to inappropriate sites, materials or abusive behaviours (and ensuring clear liability for cafes that fail to protect children).

- Blocking websites that contain child abuse images in order to deny access by potential abusers. Blocking is controversial as it raises fears about wider censorship. If used, it should remain in place only until the illegal material is removed at the source.[112] Although blocking tools are not always considered effective (images are historic, use of small secure areas of the Internet has increased, illegal content may be hosted in different countries), blocking measures may still be needed to target child abuse material.

- Taking down sites in order to remove abusive images from the Internet altogether, commonly known as 'notice and take-down'.[113] When a child abuse image site or content is identified and reported, the ISP that hosts the site is notified and is required to remove the illegal material. Moderating abusive activity on these sites represents a challenge, given the volume of material involved. Notice and take-down has proved effective in some countries, including across the EU.[114] However, despite the fact that child abuse images are illegal across many jurisdictions – which might be thought to facilitate effective take-down – their removal tends to be dealt with less speedily than other kinds of illegal Internet activity.[115] Part of the challenge lies with inadequate police resources and the priority often given to pursuit of offenders rather than preventive measures, such as the removal of sites.

- Leaving aside child abuse images, there is also a clear need for a wider set of child protection measures, such as developing strong, easy-to-use and optional security measures built into interactive forums such as chat rooms or SNS, and ensuring that the default position on safety settings is opt-out rather than opt-in.

- Filters and other types of parental control software enable parents to manage and support their child's access. Evidence shows, however, that despite this availability, just over half of parents actually activate the filtering software on their computers.[116] Some think it is activated automatically, while others believe that their children can bypass the controls. For example, the Hong Kong Council of Social Service is raising awareness of effective ways to use online filtering services and software by providing free filtering services and educating parents on their use. Even simple measures such as ensuring that a web browser is set to 'safe search' can provide added protections for children, yet few parents may know how to put that in place. The challenge for the search engine community is to determine whether to install safe search on all browsers by default, or to make much clearer how to launch it on all computers, particularly those used by children.

4. Promoting the recovery of children exposed to harm

Despite legislative, policy and protective mechanisms introduced to prevent sexual abuse and exploitation, the fact is that some children have already experienced harm and others will be harmed in the constantly evolving world of cyberspace and its interface with the offline environment. The available research on effective strategies for minimizing the impact and supporting children's recovery and rehabilitation in this context is still in its infancy. What exists has almost exclusively been undertaken in the industrialized world. However, there is sufficient knowledge of the implications of online abuse and its links with children's offline experiences to begin to identify the key strategies required to provide the necessary psychosocial support for children. While the path to abuse may be particular, good practice would entail integrating the Internet dimension into recovery systems that deal with abuse

more generally, rather than setting up specialist services. This will require:

- Treatment interventions for abused children that address building trust and that support and help children to make sense of their experience. Some children victimized by online grooming experience feelings of shame because they were 'fooled' into an online relationship with an abusive adult. Others see themselves as having autonomy and control and therefore do not recognize themselves as victims who are in need of assistance.[117] Most children abused through online grooming are conflicted; they perceive themselves as acting like an adult online, yet they continue their role as a child/young person offline.[118] Assistance to parents is also needed so they can understand their children's online experiences and offer them support.

- Child-sensitive approaches to discovery during criminal investigations that take into account the profound difficulties often experienced by children and young people in disclosing online abuse. Consideration needs to be given, for example, to ensure the proper timing and pace of interviews, recording them to avoid repeated testimony, and helping the child gain a sense of agency and control that has been denied during the experience of abuse. In response to the need to protect abused children from further trauma during the investigative process, some countries such as Canada, Iceland, the United Kingdom and the United States have adopted one-stop centres. In those centres, trained professionals from law enforcement, mental health, victim advocacy and health-care work together to gather forensic information and prevent retraumatization of victims.[119]

- Preparation for court to ensure that children understand the process, their role in the proceedings, what support will be available to them, and how to protect their confidentiality, as well as offering debriefing and counselling when court experiences have been difficult.[120]

- Treatment for young people who display sexually abusive behaviours online. Such treatment should be rooted in the same approaches used for those who commit sexually harmful acts offline. This should include a comprehensive assessment of the child and how to effectively intervene through rehabilitation and counselling; assessment of the child's development and motivation; and active involvement of parents in the process.

CONCLUSIONS

The powerful impact of the Internet on the lives of children throughout the world will continue to grow and evolve. While Internet access and child usage are highest in industrialized countries, the global pace of web access and broadband penetration, and the exponential uptake of mobile phone technologies, coupled with increasing capacities and decreasing costs, means that the rest of the world is beginning to catch up. In the next few years, it is anticipated that the most dramatic changes will occur in low- and middle-income countries.

At the moment, most of the evidence related to certain kinds of abuse comes from the industrialized world. Likewise, most of the evidence of the ways young people use the Internet and associated technologies, and the risks they face therein, comes from the same regions. Yet even there, major knowledge gaps exist. There is little information, for example, about online use by children with disabilities, cyberbullying and the challenges faced by lesbian, gay, bisexual and transgender young people. The gaps in knowledge about risk and Internet usage in Africa, as well as in most parts of Asia and the Middle East, are significant and require urgent research.

The limited research available from low- and middle-income countries, however, indicates that the issues raised in this report are globally relevant, or will soon be. For example, researchers are already learning that children from virtually all countries use SNS in largely similar ways, creating easy opportunities for potential groomers to interact with them. Children from low- and middle-income countries are less likely to use the Internet from home, and are more likely to go online from cybercafes, where they are at greater risk of encountering inappropriate images and online and offline solicitation. Lack of parental awareness and knowledge, difficult economic conditions and underdeveloped regulatory frameworks can further exacerbate potential risks and the likelihood of harm. Hence, it seems that the gaps in protection for children and young people in the online environment may be greater in low- and middle-income countries, where gaps in overall child protection already exist.

Globally, the evolution of ICT usage is at a challenging juncture. Only a small proportion of contemporary adults had access to ICT when they were children, particularly the tools that have facilitated the revolution in interaction and communication. This has probably affected the ability of adults to understand and empathize with the ways children and young people use the Internet, mobile phones and other new technologies. This may be especially true in societies where children's social activity, particularly that of adolescents, has been under fairly direct parental observation or control. Over time that situation may change, as today's computer-literate, social-networking young people become parents themselves. They may have less anxiety about the risk of exploitation and abuse because they will have been part of the generation that developed ways of handling it. On the other hand, the nature of the creativity unleashed by ICT means there will always be new elements that pose new avenues for risk that require innovative strategies for response.

Where access is widespread, ICT has in a very short period of time revolutionized the way people live their lives and interact with each other. In those places where access is expanding, these changes are currently unfolding. We know that considerable changes are still to come, but we do not yet know what those changes will be. Cyberspace throws into sharp relief the social roles and responsibilities of actors beyond the State, namely the private sector and individuals themselves. It has the potential to enrich individuals and society alike, helping to remove barriers between people, paving the way for interaction, education and development, but also presenting opportunities for wrongdoing. Children are at the forefront of this dilemma. While children and young people are intrinsic to building a safer Internet, the onus is on governments and the private sector to ensure that protection is integrated into promoting expansion of access and the positive benefits the Internet brings.

NOTES

1 European NGO Alliance for Child Safety Online, 'The Right Click: An agenda for creating a safer and fairer online environment for every child', European NGO Alliance for Child Safety Online, eNACSO, Copenhagen, June 2010, pp. 2, 5, 8, 17, available at: www.enacso.eu/images/stories/Documents/manifesto/afafinal6may.pdf, accessed 22 August 2011.

2 Lobe, B., et al. (with members of the EU Kids Online network), *Cross-National Comparison of Risks and Safety on the Internet: Initial analysis from the EU Kids Online survey of European children*, EU Kids Online, London School of Economics and Political Science, London, August 2011, p. 13.

3 United Nations General Assembly, Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, A/HRC/17/31, United Nations, New York, 21 March 2011, Guiding Principles 11 and 13 (b).

4 Livingstone, S., et al., 'Risks and Safety on the Internet: The perspective of European children, Full Findings and policy implications from the *EU Kids Online* survey of 9–16 year olds and their parents in 25 countries', EU Kids Online, London School of Economics and Political Science, London, 2011.

5 Livingstone, S. and L. Haddon, *EU Kids Online: Final report*, EU Kids Online, London School of Economics and Political Science, London (EC Safer Internet Plus Programme Deliverable D6.5), June 2009, p. 10. The study covered 21 European countries: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, France, Germany, Greece, Iceland, Ireland, Italy, Netherlands, Norway, Poland, Portugal, Slovenia, Spain, Sweden and the United Kingdom.

6 Carr, J. and Z. Hilton, *Digital Manifesto*, Children's Charities Coalition on Internet Safety, London, 2009, p. 29.

7 Carr, J., 'Briefing Note on Child Abuse Images and the Internet', Children's Charities Coalition on Internet Safety, London, July 2010, p. 2.

8 Internet Watch Foundation, *Annual and Charity Report 2010*, IWF, London, 2010, p. 1; Quayle, E. and T. Jones, 'Sexualised images of children on the internet', *Sexual Abuse*, vol. 23, no. 1, March 2011, pp. 7–21.

9 *See, for example*: Office of the Federal Ombudsman for Victims of Crime [Canada], *Every Image, Every Child: Internet-facilitated child sexual abuse in Canada*, Department of Justice, Government of Canada, 2009, p. 8, available at: www.victimsfirst.gc.ca/pdf/childp-pjuvenile.pdf; Wolok, J., D. Finkelhor and K. J. Mitchell, *Child Pornography Possessors Arrested in Internet-Related Crimes: Findings from the National Juvenile Online Victimization Study*, National Center for Missing and Exploited Children, Alexandria, VA, 2005, pp. vii, 5, 6.

10 Internet Watch Foundation, *Annual and Charity Report 2010*, IWF, London, 2010, p. 8, available at: www.iwf.org.uk/accountability/annual-reports/2010-annual-report; Internet Watch Foundation, *Annual and Charity Report 2006*, IWF, London, 2006, p. 8, www.enough.org/objects/20070412_iwf_annual_report_2006_web.pdf.

11 Internet Watch Foundation, *Annual and Charity Report 2010*, p. 8.

12 Baines, Victoria, 'Online Child Sexual Abuse: The law enforcement response – A contribution of ECPAT International to the World Congress III against Sexual Exploitation of Children and Adolescents', ECPAT International, Bangkok, November 2008, p. 2.

13 Webster, S., et al., *Scoping Report: European Online Grooming Project*, European Online Grooming Project for the European Commission Safer Internet Plus Programme, London, April 2010, p. 7. The report defines young persons as those aged 16 or younger.

14 Mitchell, Kimberly J., et al., 'Use of Social Networking Sites in Online Sex Crimes Against Minors: An examination of national incidence and means of utilization', *Journal of Adolescent Health*, vol. 47, no. 2, August 2010, pp. 183–190.

15 Webster, S., et al., *Scoping Report: European Online Grooming Project*, p. 13.

16 Ethel Quayle, 'Sexualized Images of Children on the Internet', *Sexual Abuse*, vol. 23, no. 1, March 2011, pp. 7–21.

17 Wolak, J., et al., 'Online "Predators" and their Victims: Myths, realities and implications for prevention and treatment', *American Psychologist*, vol. 63, no. 2, February–March 2008, pp. 111–128, available at: www.apa.org/pubs/journals/releases/amp-632111.pdf.

18 *See, for example*: Wolak, J., D. Finkelhor and K. J. Mitchell, *Child Pornography Possessors Arrested in Internet-Related Crimes: Findings from the National Juvenile Online Victimization Study*, National Center for Missing & Exploited Children, Alexandria, VA, 2005, available at: www.missingkids.com/en_US/publications/NC144.pdf; Sullivan, C., 'Internet Traders of Child Pornography: Profiling research', New Zealand Department of Internal Affairs, Wellington, 2005; Webb, L., J. Craissati and S. Keen, 'Characteristics of Internet Child Pornography Offenders: A comparison with child molesters', *Sex Abuse*, vol. 19, 16 November 2007, pp. 449–465; Bates A., and C.A. Metcalf, 'A Psychometric Comparison of Internet and Non-Internet Sex Offenders from a Community

Treatment Sample', *Journal of Sexual Aggression*, vol. 13, no. 1, March 2007, pp. 11–20; Baartz, D., 'Australians, the Internet and Technology-Enabled Child Sex Abuse: A statistical profile', Australian Federal Police, Canberra, Australia, 2008; Quayle, E., L. Loof and T. Palmer, 'Child Pornography and Sexual Exploitation of Children Online: A contribution of ECPAT International to the World Congress III against Sexual Exploitation of Children and Adolescents', ECPAT International, Bangkok, November 2008.

19 *See, for example*: Wolak, J., K. Mitchell and D. Finkelhor, 'Unwanted and Wanted Exposure to Online Pornography in a National Sample of Youth Internet Users', *Pediatrics*, vol. 119, no. 2, February 2007, pp. 247–257, available at: http://pediatrics.aappublications.org/content/119/2/247.full.pdf+html; Mossige, S., M. Ainsaar and C. Göran Svedin, eds., *The Baltic Sea Regional Study on Adolescents' Sexuality*, NOVA, Norwegian Ministry of Education and Research, Oslo, 2007, p. 37; Soldatova, G., 'Russian School-children as Internet Users: Types and risk groups', Foundation for Internet Development, 1999; Muhammad T., 'Danger for children at Pakistan's cafes', ECPAT newsletter No 48, July 2004, p.5, citing Pakistan Paediatric Association and Save the Children Sweden, *Exposure of children to pornography at Internet cafes of Pakistan*, 2001.

20 *See, for example*: Liao, Lih Mei, and S. M. Creighton, 'Requests for Cosmetic Genitoplasty: How should healthcare providers respond?', *BMJ*, vol. 334, no. 7603, 24 May 2007, pp. 1090–1092; and Braun, V. and L. Tiefer, 'The "Designer Vagina" and the Pathologisation of Female Genital Diversity: Interventions for change', *Radical Psychology*, vol. 8, no. 1, 2010, n.d.

21 *See, for example*: Lo, Ven-Hwei, and Ran Wei, 'Exposure to Internet Pornography and Taiwanese Adolescents' Sexual Attitudes and Behaviour', *Journal of Broadcasting & Electronic Media*, vol. 49, no. 2, June 2005, pp. 221–237; Livingstone, S., et al., *Risks and safety on the internet, Full findings*, 2011; CWIN Nepal, 'Protecting Children in Cyberspace', Kathmandu, 2009, available at: www.nta.gov.np/articleimages/file/Protecting%20Children%20in%20Cyberspace%20WTIS.pdf, accessed 21 August 2011; Rauniar, Deepak, 'Cyber Cafes of Nepal: Passage to cyber crime?', South Asia Partnership International and Bellanet Asia, Lalitpur, Nepal, March 2007; Chetty, Iyavar, and Antoinette Basson, 'Report on Internet Usage and the Exposure of Pornography to Learners in South African Schools', Film and Publication Board, Houghton, South Africa, November 2008.

22 *See, for example*: Cross, D., et al., Australian Covert Bullying Prevalence Study (ACBPS), Child Health Promotion Research Centre, Edith Cowan University, Perth, Australia; Livingstone, S., et al., *Risks and safety on the internet, Full findings 2011*; SaferNet Brasil Surveys 2009, available at: www.safernet.org.br/site/prevencao/pesquisas; Davidson, Julia, *State of the Nation Review of Internet Safety 2010*, Telecommunications Regulatory Authority, Kingdom of Bahrain, Manama, 2010; Shariff, Shaheen, *Cyber-Bullying: Issues and solutions for the school, the classroom and the home*, Routledge, London and New York, 2008; National Children's Home and Tesco Mobile, 'Putting U in the Picture: Mobile bullying survey 2005', NCH, n.d.

23 *See, for example*: Shariff, S., *Cyber-Bullying: Issues and solutions for the school, the classroom and the home*, Routledge, London and New York, 2008.

24 Livingstone, S., et al., *Risks and safety on the internet, Full findings 2011*.

25 *See*: Sharif, Shaheen, *Cyber-Bullying*.

26 *See, for example*: Keith, Susan, and Michelle E. Martin, 'Cyber-Bullying; Creating a culture of respect in a cyber world', *Reclaiming Children and Youth*, vol. 13, no. 4, Winter 2005, pp. 224–228; and Sharif, Shaheen, *Cyber-Bullying*.

27 Raskauskas, Juliana, and Ann D. Stoltz, 'Involvement in Traditional and Electronic Bullying among Adolescents', *Developmental Psychology*, vol. 43, no. 3, May 2007, pp. 564–575.

28 *See, for example*: Hasebrink, U., et al., *Patterns of risk and safety online: In-depth analyses from the* EU Kids Online survey *of 9-16-year olds and their parents in 25 countries*, London School of Economics and Political Science, London: EU Kids Online, August 2011, pp. 7, 22, 31.

29 International Telecommunication Union, 'Use of Information and Communication Technology by the World's Children and Youth: A statistical compilation', ITU, Geneva, June 2008; Lenhart, A., et al., 'Social Media & Mobile Internet Use Among Teens and Young Adults', Pew Internet & American Life Project, Washington, D.C., 2010.

30 Livingstone, S. and L. Haddon, *EU Kids Online: Final report 2009*, p. 5.

31 Livingstone, S., et al, *Risks and Safety on the Internet, Full findings*, p. 31.

32 International Telecommunication Union, 'Use of Information and Communication Technology by the World's Children and Youth ; Livingstone, S. and L. Haddon, *EU Kids Online: Final report 2009*.

33 Safer Internet Programme, *Eurobarometer, Towards a safer use of the Internet for children in the EU – A parents' perspective*, Eurobarometer, European Commission, Brussels, December 2008, p. 13.

34 Livingstone, S., et al., *Risks and Safety on the Internet, Full findings*, p. 26.

35 Davidson, J. and E. Martellozzo, *State of the Nation Review of Internet Safety 2010*, Telecommunications Regulatory Authority, Kingdom of Bahrain, Manama, 2010, available at: www.tra.org.bh/en/pdf/SafeSurf_TRA_Report.pdf, accessed 7 September 2011.

36 Chetty, Iyavar, and Antoinette Basson, 'Report on Internet Usage and the Exposure of Pornography to Learners in South African Schools', Film and Publication Board, Houghton, South Africa, November 2006, p. 23.

37 Center of Studies on Information and Communication Technologies, 'Survey on the Use of Information and Communication Technologies in Brazil 2009', CETIC.br, Brazil Internet Steering Committee, São Paolo, 2010, p. 227, available at: www.cetic.br/english/. This percentage includes individuals who declared having accessed the Internet at least once in their lives from any location.

38 ITU, 'Use of Information and Communication Technology by the World's Children and Youth', pp. 29, 41.

39 Symantec, 'Norton Online Living Report 09', Mountain View, CA, 2009, pp. intro, 4, 13, 14. The countries surveyed were Australia, Brazil, Canada, China, France, Germany, India, Italy, Japan, Sweden, the United Kingdom and the United States; the survey is available at: www.protegiendoles.org/documentacion/estante4/NOLR_Report_09.pdf, accessed 19 August 2011.

40 International Telecommunication Union, 'The World in 2010: ICT facts and figures', ITU, Geneva, 2010, pp. 4–5; available at:www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf,accessed 26 August 2011.

41 Center of Studies on Information and Communication Technologies, 'Survey on the Use of Information and Communication Technologies in Brazil 2009', CETIC.br, 2009; pp. 54, 133, 239.; Center of Studies on Information and Communication Technologies, 'Survey on the Use of Information and Communication Technologies in Brazil 2008', CETIC.br, 2008; p. 228; Center of Studies on Information and Communication Technologies, 'Survey on the Use of Information and Communication Technologies in Brazil 2006', CETIC.br, 2006, p. 113.

42 Data provided by the Japanese Delegation to the OECD , Organisation for Economic Co-operation and Development, *The Protection of Children Online: Risks faced by children online and policies to protect them*, OECD Digital Economy Papers, No. 179, OECD Publishing, Paris, May 2011, p. 10; and Eurobarometer 2008, annex tables and survey details, Towards a safer use of the Internet for children in the EU – A parents' perspective, analytical report, table 21b, p. 112.

43 ITU, *Use of Information and Communication Technology by the World's Children and Youth*, 2008, p. 33. Chapter 5, p. 19 of the report includes the following classifications: *Children* refers to individuals in the age group 5–14 or younger; and *Youth* refers to individuals in the age group 15–24.

44 Lenhart, A., et al., 'Social Media & Mobile Internet Use Among Teens and Young Adults', Pew Internet & American Life Project, Washington, D.C., 2010, available at: http://pewresearch.org/pubs/1484/social-media-mobile-internet-use-teens-millennials-fewer-blog, accessed 9 June 2011.

45 Livingstone, S., et al., *Risks and Safety on the Internet, Full findings*, p. 5, available at: www2.cnrs.fr/sites/en/fichier/rapport_english.pdf, accessed 12 October 2011.

46 Socialbakers.com, 'India Facebook Statistics, Penetration, Demography', Socialbakers Ltd., www.socialbakers.com/facebook-statistics/india#chart-intervals, accessed on 12 October 2011.

47 Socialbakers.com, 'Brazil Facebook Statistics', Socialbakers Ltd., www.socialbakers.com/facebook-statistics/brazil, accessed on 12 October 2011.

48 Byron, T., *Safer Children in a Digital World: The Report of the Byron Review*, Department for Children, Schools and Families, Annesley, UK, March 2008, available at: http://media.education.gov.uk/assets/files/pdf/s/safer%20children%20in%20a%20digital%20world%20the%202008%20byron%20review.pdf.

49 *See, for example*: Davidson, J., E. Martellozzo and M. Lorenz, 'Evaluation of CEOP ThinkUKnow Internet Safety Programme and Exploration of Young People's Internet Safety Knowledge', Centre for Abuse & Trauma Studies, Kingston University, London, July 2009, available at:http://cats-rp.org.uk/pdf%20files/Internet%20safety%20report%204-2010.pdf, accessed 21 August 2011; Davidson, J. C. and E. Martellozzo, 'Educating children about sexual abuse and evaluating the Metropolitan police safer surfing programme', Project Report, Metropolitan Police, London, 2004; Donath, J., and d. boyd, 'Public displays of connection', *BT Technology Journal*, vol. 22, no. 4, October 2004, pp. 71–82, available at: www.danah.org/papers/PublicDisplays.pdf; and Child Exploitation and Online Protection Centre, 'Understanding Online Social Network Services and Risks to Youth: Stakeholder perspectives – A preliminary report on the findings of the CEOP Centre's social network seminar series', Child Exploitation and Online Protection Centre, London, 2006.

50 Donath, J., and d. boyd, 'Public displays of connection'.

51 *See, for example*: Davidson, J., E. Martellozzo and M. Lorenz, 'Evaluation of CEOP ThinkUKnow Internet Safety Programme; International Youth Advisory Congress (A CEOP led VGT initiative), 'IYAC Children and Young Persons' Global Online Charter Supplementary Document', Child Exploitation and Online Protection (CEOP) Centre, London, 2008.

52 Lobe, B., et al. (with members of the EU Kids Online network), *Cross-National Comparison of Risks and Safety on the internet: Initial analysis from the EU Kids Online survey*.

53 *See, for example*: SaferNet Brasil Surveys, 2009; and Davidson, J., *State of the Nation Review of Internet Safety 2010*, p. 4.

54 *See, for example*: van der Gaag, Nikki, *Because I Am a Girl: The State of the World's Girls 2010 – Digital and urban frontiers: Girls in a changing landscape*, Plan International, Brussels, 2010, available at: <http://plan-international.org/girls/resources/digital-and-urban-frontiers-2010.php>, accessed 27 August 2011; SaferNet Brasil Surveys, 2009; Lenhart, A., et al., 'Social Media & Mobile Internet Use Among Teens and Young Adults', Pew Internet & American Life Project, Washington, D.C., 2010, p. 8; CWIN Nepal, 'Protecting Children in Cyberspace'.

55 *See*: Lenhart, A., 'Teens and Sexting: How and why minor teens are sending sexually suggestive nude or nearly nude images via text messaging', Pew Internet & American Life Project, Washington, D.C., 15 December 2009, available at www.pewinternet.org/~/media//Files/Reports/2009/PIP_Teens_and_Sexting.pdf.

56 Lenhart, A., *Teens and Sexting, and SaferNet Brasil Surveys*, 2009.

57 Ybarra, M. L., and K. J. Mitchell, 'How Risky Are Social Networking Sites?: A comparison of places online where youth sexual solicitation and harassment occurs', *Pediatrics*, vol. 121, no. 2, 1 February 2008, pp. e350–e357; available at: http://pediatrics.aappublications.org/content/121/2/e350.

full, accessed 26 August 2011; Ybarra, M. L., et al., 'Internet Prevention Messages: Targeting the right online behaviors', *Archives of Pediatric and Adolescent Medicine*, vol. 161, no. 2, February 2007, pp. 138–145, available at: http://archpedi.ama-assn.org/cgi/content/full/161/2/138.

58 Optem, 'Safer Internet for Children: Qualitative study in 29 European countries – Summary report', Eurobarometer, Brussels, May 2007, available at: http://ec.europa.eu/public_opinion/archives/quali/ql_safer_internet_summary.pdf.

59 Ybarra, M. L., et al., 'Internet Prevention Messages', pp. 138–145.

60 *See, for example*: UNICEF Regional Office for West and Central Africa, 'Promoting Synergies between Child Protection and Social Protection: West and Central Africa', Overseas Development Institute and United Nations Children's Fund, London and Dakar, 2009, available at: www.odi.org.uk/resources/details.asp?id=3477&title=child-protection-social-protection-west-central-africa.

61 Mitchell K. J., D. Finkelhor and J. Wolak, 'Risk factors for and impact of online sexual solicitation of youth', *The Journal of the American Medical Association*, vol. 285, no. 23, 20 June 2001, pp. 3011–3014; Dawes, A. and A. Govender, 'The Use of Children in Pornography in South Africa', Human Sciences Research Council, Pretoria, 2007, available at: www.hsrc.ac.za/Research_Project-796.phtml.

62 Livingstone, S., 'e-Youth: (Future) policy implications – Reflections on online risk, harm and vulnerability', Presentation at 'e-Youth: balancing between opportunities and risks' (26–28 May 2010, Antwerp, Belgium), London School of Economics Research Online, London, June 2010, available at: http://eprints.lse.ac.uk/27849/.

63 van der Gaag, Nikki, *Because I Am a Girl: The State of the World's Girls 2010*.

64 van der Gaag, Nikki, *Because I Am a Girl: The State of the World's Girls 2010*; Bawagan, Aleli, and Anjanette Saguisag, 'The Role of the Private Sector, particularly ISPs and Internet Cafe Owners, as Active Partners in Protecting Children from Sexual Abuse and Exploitation in the Philippines: An on-going case study by UNICEF Philippines', UNICEF, Makati City, Philippines, n.d., available at: <www.unicef-irc.org/files/documents/d-3600-Working-with-internet-ser.pdf>, accessed 21 August 2011; Plan India, 'Girls in a Changing Landscape: Urban and digital frontiers – The state of the girl child in India 2010', New Delhi, September 2010.

65 *See, for example*: Long Island Network of Community Services/BiasHELP, 'STOPtechNObullying: LGBTQ – Lesbian, gay, bisexual, transgender and questioning youth', Hauppauge, New York, 2011, available at: http://stoptechnobullying.org/lgbtq.php, accessed 22 August 2011; and Shariff, Shaheen, *Cyber-Bullying*.

66 'Understanding social networking services and risks to youth, Stakeholder perspectives', a preliminary report on the findings of the CEOP centre's social network seminar series, Child Exploitation and Online Protection Centre, London, 2006; SaferNet Brasil Surveys 2009, available at: www.safernet.org.br/site/prevencao/pesquisas

67 Child Exploitation and Online Protection Centre, 'Understanding Social Networking Services and Risks to Youth: Stakeholder perspectives – A preliminary report on the findings of the CEOP Centre's Social Network Seminar Series', CEOP, London, 2006, available at: www.ceop.police.uk/Documents/socialnetwork_serv_report_221206.pdf.

68 'Staying Safe Survey 2009: Young people and parents' attitudes around Internet safety', Department for Children, Schools and Families, Government of the United Kingdom, Runcorn, UK, December 2009; Livingstone, S. and L. Haddon, *EU Kids Online: Final report*.

69 Livingstone, S. and L. Haddon, *EU Kids Online: Final report*.

70 *See, for example*: Davidson, J., *State of the Nation Review of Internet Safety 2010*; Staksrud, E. and S. Livingstone, 'Children and Online Risk: Powerless victims or resourceful participants?', *Information, Communication & Society*, vol. 12, no. 3, 2009, pp. 364–387; Gallup Organisation, 'Towards a Safer Use of the Internet for Children in the EU' (Eurobarometer), http://ec.europa.eu/public_opinion/flash/fl_248_en.pdf.

71 'Staying Safe Survey 2009: Young people and parents' attitudes around Internet safety'; and Livingstone, S. and L. Haddon, *EU Kids Online: Final report*.

72 Cho, Chang-Hoan and Hongsik John Cheon, 'Children's Exposure to Negative Internet Content: Effects of family context', *Journal of Broadcasting & Electronic Media*, 1 December 2005, pp. 488–509.

73 *See*: Staksrud, E. and S. Livingstone, 'Children and Online Risk'.

74 *See, for example*: Voices of Youth, 'Survey on Internet Use, 2010' (internal document), United Nations Children's Fund, New York; van der Gaag, Nikki, *Because I Am a Girl: The State of the World's Girls 2010*.

75 *See*: Davidson, J., E. Martellozzo and M. Lorenz, 'Evaluation of CEOP ThinkUKnow Internet Safety Programme and Exploration of Young People's Internet Safety Knowledge'.

76 Livingstone, S., et al., *Risks and safety on the internet, Full findings 2011*.

77 *For a comprehensive overview of legal frameworks, see*: Newell, P., 'Legal Frameworks for Combating Sexual Exploitation of Children', UNICEF Innocenti Research Centre, Florence, 2008.

78 Third World Congress against Commercial Sexual Exploitation of Children, 'The Rio de Janeiro Declaration and Call for Action to Prevent and Stop Sexual Exploitation of Children and Adolescents', 2008, p. 6, available at: www.ecpat.net/WorldCongressIII/PDF/Outcome/WCIII_Outcome_Document_Final.pdf, accessed 7 September 2011.

79 United Nations, Report of the independent expert for the United Nations study on violence against children, A/61/299, United Nations General Assembly, New York, 29 August 2006, p. 32, para. 114 (j).

80 International Centre for Missing & Exploited Children, 'Child Pornography: Model legislation & global review', 6th ed., ICMEC, Alexandria, VA, 2010. Information available at: www.icmec.org/missingkids/servlet/PageServlet?LanguageCountry=en_X1&PageId=4346, accessed 22 September 2011.

81 European Commission, 'Proposal for a Directive on Combating Sexual Abuse, Sexual Exploitation of Children and Child Pornography, repealing Framework Decision 2004/68/JHA', European Commission, Brussels, 29 March 2010, available at: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/107.

82 European Union, Legislative Acts and Other Instruments – Directive of the Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, European Union, Brussels, 4 November 2011. Also see: Council of the European Union, 'EU takes action to combat sexual abuse of children and child pornography', press release, Council of the European Union, Brussels, 15 November 2011.

83 GSMA, *Mobilising Europe's Digital Agenda*, GSMA, London, 2010, www.gsmworld.com/our-work/public-policy/gsma_europe/mobilising/downloads/GSMA_UmbrellaStory_A5Brochure.pdf; GSM World, European Framework (webpage), *see*: www.gsmworld.com/our-work/public-policy/framework_mobile_use_younger_teenagers_children.htm.

84 Donoso, V., *Results of the Assessment of the Implementation of the Safer Social Networking Principles for the EU. Individual Reports of Testing of 14 Social Networking Sites*, European Commission, Safer Internet Programme, Luxembourg, May 2011, available at: http://ec.europa.eu/information_society/activities/social_networking/eu_action/implementation_princip_2011/index_en.htm. *Also see*: Donoso, V., *Assessment of the implementation of the Safer Social Networking Principles for the EU on 14 websites: Summary report*, European Commission, Safer Internet Programme, Luxembourg, 2010.

85 'Memorandum on the Protection of Personal Data and Privacy in Internet Social Networks, Specifically in Regard to Children and Adolescents', 2009, PDF available, in order of language, in Spanish, Portuguese, English and French, www.iijusticia.org/esp_port_eng_fran.pdf, accessed 30 August 2011.

86 Gregorio, Carlos, 'Sexual Abuse and Exploitation in the Converged Online/Offline Environment: A point of view from Latin America', unpublished document; InSafe *Annual Report 2010*, InSafe, Brussels, October 2010.

87 *See, for example*: Wall, David S., 'The Internet as a Conduit for Criminal Activity', Chapter 4 in April Pattavina, ed., *Information Technology and the Criminal Justice System*, Sage Publications, Thousand Oaks, CA, 2005, pp. 77–98, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=740626, accessed 7 September 2011.

88 Stephens, Gene, 'Policing the Future: Law enforcement's new challenges', *The Futurist*, March–April 2005, pp. 51–57, www.policefuturists.org/pdf/M-A2005Futurist_Stephens.

89 Palmer, T., 'Sexual abuse and exploitation in the converged online/offline environments: Referral services and rehabilitation, (unpublished paper for the UNICEF Innocenti Research Centre).

90 *See, for example*: Palmer, Tink, 'Behind the Screen: Children who are the subjects of abusive images', in Quayle, Ethel and Maxwell Taylor, eds., *Viewing Child Pornography on the Internet: Understanding the offence, managing the offender, helping the victims*, Russell House Publishing, Lyme Regis, UK, 2005; Palmer, T. and L. Stacey, *Just One Click: Sexual abuse of children and young people through the Internet and mobile phone technology*, Barnardo's, Ilford, UK, 2004; Von Weiler, Julia, Annette Haardt-Becker and Simone Schulte, 'Care and Treatment of Child Victims of Child Pornographic Exploitation (CPE) in Germany', *Journal of Sexual Aggression*, vol. 16, no. 2, July 2010, pp. 211–222.

91 Palmer, T., 'Sexual Abuse and Exploitation in the Converged Online/Offline Environments: Referral services and rehabilitation', 2010 (unpublished paper prepared for the UNICEF Innocenti Research Centre).

92 Quayle, E, L. Loof and T. Palmer, 'Child pornography and exploitation of children online. A contribution of ECPAT International to the World Congress III against Sexual Exploitation of Children and Adolescents', ECPAT International, Bangkok, 2008.

93 Microsoft Corporation, *Microsoft 2010 Corporate Citizenship Repor*t, Microsoft Corporation, Redmond, VA, 2010, p. 47 ; Cornell University Law School, Legal Information Institute, *Use to combat child pornography of technical elements relating to images reported to the CyberTipline*, U.S. Code, Title 18, Part 1, Chapter 110, No. 2258C, available at: www.law.cornell.edu/uscode/usc_sec_18_00002258---C000-.html.

94 Maalla, N. M. 'Report of the Special Rapporteur on the sale of children, child prostitution and child pornography', A/HRC/12/23, United Nations, New York, 13 July 2009, p. 12; available at <www.unhcr.org/refworld/docid/4ab0d35a2.html>, accessed 1 September 2011.

95 Nissenbaum, H., 'The Meaning of Anonymity in an Information Age', *The Information Society*, vol. 15, 1999, pp. 141–144, available at: www.nyu.edu/projects/nissenbaum/paper_anonimity.html, accessed 22 September 2011.

96 Farfinski, S., *UK Cybercrime Report*, Garlik, Richmond, UK, n.d., available at www.garlik.com/press/Garlik_UK_Cybercrime_Report.pdf.

97 *See, for example:* Police Commissioners' Conference Electronic Crime Working Party, 'The Virtual Horizon: Meeting the law enforcement challenges – Developing an Australasian law enforcement strategy for dealing with electronic crime', ACPR-RS-134.1, Australasian Centre for Policing Research, Payneham, Australia, 2000.

98 Interview with the Child Exploitation and Online Protection Centre, March 2011.

99 Von Weiler, J., A. Haardt-Becker and S. Schulte, 'Care and Treatment of Child Victims of Child Pornographic Exploitation (CPE) in Germany', *Journal of Sexual Aggression*, vol. 16, no. 2, July 2010, pp. 211–222. Berggrav, S., Omsorg på nettet: Er det mitt ansvar?, Barnevernets utfordringer i å møte overgrepp på internett, Redd Barna (*Care on the Internet: Is it my responsibility? The challenges of the Child Welfare Services in meeting online abuse*, Save the Children Norway), Oslo, 2010.

100 Palmer, T., 'Sexual Abuse and Exploitation in the Converged Online/Offline Environments' (unpublished paper prepared for the UNICEF Innocenti Research Centre).

101 Survey conducted in September 2010 by Tink Palmer, United Kingdom for the purposes of this paper.
102 SaferNet Brasil, 'Nética: Ethics and education for developing cyber-citizenship in Brazil', 2010, http://files.eun.org/insafe/blog/Netica.doc, accessed 31 August 2011.
103 Child Protection Partnership (CPP) Digital Literacy Initiative, in collaboration with IICRDTrend Microsystems and Certiport Implementation by The Aspire Group Company (TAGC), 2010 (unpublished document).
104 Odhiambo, Victoria, 'Youth Mobilization to Promote Codes of Conduct in Internet Cafes in Africa', Presentation for Corporate Engagement in IT Companies Seminar, ECPAT World Congress III, Rio de Janeiro, 27 November 2008; available at: www.ecpat.net/WorldCongressIII/PDF/Publications/T4_WS3c.pdf, accessed 31 August 2011.
105 Sharif, S., *Cyber-Bullying*, p. 256.
106 International Centre for Missing & Exploited Children, 'Child Pornography: Model legislation & global review'.
107 Human Rights Council, 'Joint Report of the Special Rapporteur on the Sale of Children, Child Prostitution and Child Pornography, and the Special Representative of the Secretary-General on Violence against Children', A/HRC/16/56, United Nations, New York, 7 March 2011, available at http://srsg.violenceagainstchildren.org/document/a-hrc-16-56_204.
108 International Centre for Missing & Exploited Children, 'Child Pornography: Model legislation & global review'.
109 International Criminal Police Organization, 'Notices & Diffusions', INTERPOL, Lyon, France, 22 June 2011, available at: www.interpol.int/Public/Notices/default.asp, accessed 2 September 2011.
110 United Nations Economic and Social Council, 'Guidelines on Justice Matters involving Child Victims and Witnesses of Crime', Resolution 2005/20, United Nations, New York, 22 July 2005.
111 Few of the codes of good practice developed within the United Kingdom under the auspices of the Home Secretary's Task Force on Child Internet Safety had any monitoring provisions attached to them. This approach was expressly rejected in a review conducted in 2008 by Professor Tanya Byron, available at: www.education.gov.uk/ukccis/about/a0076277/the-byron-reviews, and further endorsed by the Bailey Review, www.education.gov.uk/inthenews/inthenews/a0077662/bailey-review-of-the-commercialisation-and-sexualisation-of-childhood-final-report-published.
112 Internet Watch Foundation, *2009 Annual and Charity Report*, IWF, Cambridge, UK, 2009, available at: www.iwf.org.uk/assets/media/annual-reports/IWF%202009%20Annual%20and%20Charity%20Report.pdf.
113 Moore, T. and R. Clayton, 'The Impact of Incentives on Notice and Take-Down', in *Managing Information Risk and the Economics of Security*, Springer, New York, 2009, pp. 199–223.
114 *See, for example*: Using blocking to combat online child abuse images: Questions & Answers, Q3. Can't sites known to contain child abuse images just be taken down, as they are illegal?, European NGO Alliance for Child Safety Online.
115 Moore, T. and R. Clayton, 'The Impact of Incentives on Notice and Take-Down'.
116 Ofcom's Submission to Safer Children in A Digital World, p. 95.
117 Nyman, Anders, *Abused Online*, BUP Elefanten (Child and Adolescent Psychiatric Unit) and the County Council of Östergötland, n.d. ; Palmer T., 'Sexual abuse and exploitation in the converged online/offline environments' (unpublished paper prepared for the UNICEF Innocenti Research Centre).
118 Palmer T., 'Sexual abuse and exploitation in the converged online/offline environments' (unpublished paper prepared for the UNICEF Innocenti Research Centre).
119 *See, for example*: Office of the Federal Ombudsman for Victims of Crime [Canada], *Every Image, Every Child*, p. 30.
120 Lansdown, G., Article 12: *The Right of the Child to be Heard: A resource book for governments*, UNICEF/Save the Children/OHCHR, London, forthcoming.

© Bjoern Steinz / Panos Pictures

ACRONYMS

CEOP	Child Exploitation and Online Protection Centre (United Kingdom)
ECPAT	End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes
EU	European Union
ICT	information and communication technology
INTERPOL	International Criminal Police Organization
IRC	Innocenti Research Centre (UNICEF)
ISP	Internet service provider
ITU	International Telecommunication Union
IWF	Internet Watch Foundation
LGBT	lesbian, gay, bisexual and transgender (people)
OPSC	Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography
SNS	social networking site

GLOSSARY

Terms relating to sexual abuse and exploitation of children

child – Every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier (article 1, Convention on the Rights of the Child).

child abuse images – 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 (*see 'child pornography' below*). Although there is no internationally agreed definition of 'child abuse images', this report uses the term as defined above and is preferred over child pornography because it leaves no doubt that abuse and exploitation are involved.

child pornography – 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 (article 2, Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography). In this report, the term 'child abuse images' is preferred.

child prostitution – Use of a child in sexual activities for remuneration or any other form of consideration (article 2, Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography).

child sexual abuse – As defined in article 18 of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201, also known as 'the Lanzarote Convention'):

(a) Engaging in sexual activities with a child who, according to the relevant provisions of national law, has not reached the legal age for sexual activities;

(b) Engaging in sexual activities with a child where:

- use is made of coercion, force or threats;
- abuse is made of a recognized position of trust, authority or influence over the child, including within the family;
- abuse is made of a particularly vulnerable situation of the child, notably because of a mental or physical disability or a situation of dependence.

The provisions of paragraph (a) are not intended to govern consensual sexual activities between minors [children under 18 years old] (article 18.3).

child sexual exploitation – Child prostitution, child pornography and the participation of a child in pornographic performances, including recruiting, coercing or causing a child to participate in pornographic performances, or profiting from or otherwise exploiting a child for such purposes and knowingly attending performances involving the participation of children; intentionally causing a child who has not reached the legal age for sexual activities to witness sexual abuse or sexual activities, even without having to participate; and the solicitation of children for sexual purposes (Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, articles 18–23).

online child sexual abuse – Production, distribution, downloading or viewing of child abuse material (both still and video images), also known as child pornography; online solicitation of children and young people to produce self-generated child abuse material, to engage them in sexual chat or other online sexual activity, or to arrange an offline meeting for the purposes of sexual activity, also known as grooming or luring; and facilitation of any of the above. There is no agreed definition of online child sexual abuse in international law; for the purposes of this report, the term is defined as noted above.

online grooming – Defined by various authors and used in this report to describe a process intended to lure children into sexual behaviour or conversations with or without their knowledge, or a process that involves

communication and socialization between the offender and the child in order to make him or her more vulnerable to sexual abuse. The term 'grooming' has not been defined in international law; some jurisdictions, including Canada, use the term 'luring'.

online/offline environment – The interface between computer-mediated communication and face-to-face communication. 'Online' entails non-physical communication and 'offline' involves physical interaction.

paedophile – A diagnostic category referring to an exclusive sexual orientation towards prepubescent children. It does not accurately portray those who sexually abuse children via the Internet and mobile technology, many of whom are married or in long-term sexual relationships with adults. Therefore, in this report, the terms 'child abuser' or 'sexual abuser' are used.

sale of children – Any act or transaction whereby a child is sold by any person or group of persons to another for remuneration or any other consideration (Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, article 2(a)).

sexual abuser – Anyone who sexually offends against children or engages in any sexual activity with a child, commonly called a 'paedophile', but as noted above, the terms 'child abuser' or 'sexual abuser' are more appropriate. There is no internationally agreed definition of this term.

solicitation of children for sexual purposes – The intentional proposal, through information and communication technologies, of an adult to meet a child who has not reached the legal age for sexual activities, for the purpose of engaging in sexual activities or the production of child pornography (adapted from Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, article 23).

Terms relating to the online environment

blog – Websites that have entries, or 'posts', including text and images, typically displayed in chronological order. Entire blogs or particular posts can be public and available to everyone online, or private and available only to users who are authorized by the blog owner/author.

broadband – A high-capacity digital connection that facilitates a faster Internet connection and enables a more rapid exchange of larger files such as videos, games and software applications.

browser – A software program that is selected by the consumer and used to locate and display pages on the World Wide Web (web pages). Popular browsers include Microsoft's Windows Internet Explorer, Firefox, Google Chrome, Safari and Opera.

chat room – Virtual 'meeting rooms' where people can communicate by typing in messages to each other, or chat, in real time. Most chat rooms focus on a particular topic, but some are more general and are created to provide a forum for individuals to meet other people.

cyberspace – The virtual shared universe of the world's computer networks. The term was created by William Gibson in his 1984 novel *Neuromancer*. It is often used interchangeably with 'the Internet'.

download – The process in which data are copied to a computer from the Internet or another source such as an external drive, a disk, a phone or other devices. Data that are typically downloaded on to a computer for viewing, storage and future access include text files, photographs, videos and music.

email – Short for 'electronic mail', a tool that allows someone to send a message, or 'email', to another person's electronic mailbox over a communications network such as the Internet.

filter – A mechanism to sift out and block access to certain material. Most child-safety software packages use a filtering component; the program may be designed to operate on an individual personal computer or it may be applied to a network of computers. Often a filtering component is provided 'free' as an integral part of a computer's operating system, or it will come as part of a connectivity package from a user's Internet service provider. Customized filters have also been developed for mobile phones and consoles.

information and communication technology (ICT) – Any communication device or application, encompassing radio, television, cellular phones, satellite systems, and computer and network hardware and software, as well as associated services and applications such as videoconferencing and distance learning.

instant messaging (IM) – Text-based communications service similar to a chat room. The key difference is that chat rooms are usually public spaces where anyone can participate, while IM systems generally rely on a 'buddy list' or some other list of people predetermined by the user. Only people on the list can communicate with the user, hence each user has control over whom he or she includes in instant messaging. Google Chat, MSN and Twitter are examples of IM services; most social networking sites (*see definition below*) have an IM function.

(the) Internet – Worldwide network of hundreds of thousands of interconnected computer networks, using a common set of communication protocols and sharing a common addressing scheme. The Internet facilitates the transmission of email messages, text files, images and many other types of information between computers.

Internet service provider (ISP) – A commercial enterprise that provides users with direct access to the Internet, usually for a fee, or a business that provides Internet services such as website hosting or development.

online – Controlled by or connected to a computer network or the Internet, and any activity or service that is available on or carried out via the Internet. A person is 'online' when she or he has logged into a network of computers, or has connected a computer or other device to the Internet. The term 'offline' describes activity that is not carried out online as well as the condition of being disconnected from the Internet.

peer-to-peer (P2P) – Software that allows transmission of data directly from one computer to another over the Internet, usually without needing to involve a third-party server.

penetration – How widely a technology gets adopted among people to whom the technology is available.

photo sharing – An application that enables users to upload, view and share photos; users can allow either public or private access.

sexting – A form of text messaging/texting (*see definition below*) in which people send pictures of a sexual nature or sexually explicit text. This is especially common among teenagers.

short message service (SMS) – The common text messaging service available on mobile phones, other handheld devices and computers.

smartphones – Mobile phones that incorporate a complete operating system and are able to access the Internet. In many ways, they are like tiny computers, with more memory and bigger screens than ordinary phones.

social media – Primarily Internet- and mobile-based tools for sharing and discussing information. 'Social media' most often refers to activities that integrate technology, telecommunications and social interaction, and are used to share words, pictures, videos and audio.

social networking sites (SNS) – Online utilities that enable users to create profiles, public or private, and form a network of friends. SNS allow users to interact with friends via private and public means, such as messages and instant messaging, and to post user-generated content, such as photos and videos. Examples of SNS include Facebook, MXit, Myspace and Orkut.

text messaging/texting – Short text messages sent using mobile phones, wireless handheld devices (such as Sidekick) and personal digital assistants (basic handheld computers known as 'PDAs').

upload – The process of transmitting data from a user's machine to a server.

video sharing – Like photo sharing (*see above*) but for videos. These videos are often user-generated; the largest video sharing website is YouTube.

virtual worlds – Online simulated three-dimensional environments inhabited by players who interact with each other via avatars (movable icons representing a person in cyberspace). Second Life, or more popularly with young people, Teen Second Life, are examples of virtual worlds.

webcam – A video camera that is built into or connected to a computer that is connected to the Internet.

World Wide Web (WWW) – A hypertext-based system for finding and accessing data on the Internet. The Web hosts documents, called web pages, which may be linked with other documents or information systems. The Web is a portion of the Internet and not all servers on the Internet are part of the Web.

UNICEF Innocenti Research Centre
Piazza SS. Annunziata, 12
50122 Florence, Italy
Tel: (39) 055 20 330
Fax: (39) 055 2033 220
florence@unicef.org
www.unicef-irc.org

ISBN: 978-88-6522-004-7
IRC stock no: 645U

Front cover photo: © UNICEF/NYHQ2010-3011/Pirozzi