Child Safety Online
Global challenges and strategies
Technical Report
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.

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

A printed summary of this technical report is available from the address below and can be downloaded from the Innocenti Research Centre website.

Correspondence and requests for permission to reproduce or translate UNICEF IRC publications 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

Front cover photo: © UNICEF/NYHQ2010-3011/Giacomo Pirozzi
Design and layout: BlissDesign.com

© United Nations Children’s Fund (UNICEF)
May 2012

Child Safety Online: Global challenges and strategies

Technical Report
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/peer 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 Petersberg, Russian Federation
Rodrigo Nejm, Director of Prevention Programmes, SaferNet Brasil
Sonia Livingstone, Coordinator EU Kids Online; Professor and Head of the 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
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 effortlessly 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, despite children’s agency, 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
# CONTENTS

Acknowledgements ..................................................................... ii  
Foreword ................................................................................... iii  
Introduction .................................................................................. 1  
Scope, methodology and limitations ........................................... 3  

## PART ONE: CHILD PROTECTION IN THE ONLINE/OFFLINE ENVIRONMENT ................................. 9  
Chapter 1: Understanding the social and cultural context .................. 10  
Chapter 2: Sexual exploitation and abuse in the online/offline environment ............................ 13  
  Child abuse images .................................................................... 13  
  Grooming .................................................................................... 15  
  Abusers and exploiters online ...................................................... 16  
Chapter 3: Children’s activities using information and communication technology ................... 18  
  Levels of Internet access and usage ............................................. 19  
  Use of mobile phones .................................................................... 21  
  Children’s online and cyberspace activities .................................. 22  
Chapter 4: Risk, vulnerability and harm ........................................... 26  
  Behaviour and activities carrying potential risk of harm .................. 26  
  Exposure to pornography .......................................................... 31  
  Bullying and harassment ............................................................ 33  
  Perceptions of risk, vulnerability and harm .................................... 35  
  Vulnerability to sexual solicitation ............................................. 39  
  Potential impact .......................................................................... 42  
Chapter 5: Sources of support and help ........................................... 44  

## PART TWO: ONLINE/OFFLINE PROTECTION ................................................................. 49  
Chapter 6: International instruments and commitments .......................... 50  
  Convention on the Rights of the Child .......................................... 51  
  Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography ......................... 54  
  UN Trafficking Protocol .............................................................. 54  
  Council of Europe Convention on Cybercrime ............................. 54  
  Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse ........................................ 55  
  Commitments by the international community .............................. 55  
Chapter 7: Challenges for law enforcement and child protection .................. 59  
  National legislation ....................................................................... 59  
  Law enforcement and child protection ......................................... 61  
Chapter 8: Building a protective environment: Implications for policy response .................... 70  
  Objective One: Empower children and enhance resilience to harm ....... 71  
  Objective Two: Remove impunity for abusers ............................... 77  
  Objective Three: Reduce availability and access to harm ................ 85  
  Objective Four: Promote recovery and rehabilitation for children exposed to harm ....................... 90  
Conclusions ............................................................................... 95  
Glossary ....................................................................................... 97  
Notes ......................................................................................... 102  
Abbreviations and acronyms ......................................................... 129
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 20 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 technologies (ICT) have not created crimes involving sexual abuse and exploitation of children, they have 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. 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 play a role is only an issue for the economically better off, whether societies or social groups. Web access is rapidly increasing, 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 speeds start to become available in lower-income countries there is a high expectation that, in the absence of any counter 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, which 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 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. 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 about how the Internet should operate, or in relation to 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 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 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. 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 might 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 impact 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 nondiscrimination 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. 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, both in 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 information and communication technologies 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 crime 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 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 multi-tiered 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.

**Scope, methodology and limitations**

The initial focus of research was to gather evidence on the impact of sexual abuse and exploitation in the online/offline world. Cyberbullying is also included because numerous surveys show this phenomenon to be a concern of children and young people. The key areas include:
(a) The current available evidence on the behaviour and activities of children and young people online in order to gain a better understanding of the relationship between the online and offline environments and the risks and potential for violence and sexual abuse and exploitation as a consequence of that interface. The goal of prevention and behavioural change in relationship to sexual exploitation and abuse of children in the online/offline environment cannot be pursued effectively without confronting such fundamental questions as:

- How are children and young people using and exploring the new information technologies? How are these information technologies influencing them?
- What are the current behaviour patterns of children?
- What risks do they currently face? How do those risks arise, and how do children mitigate those risks?
- To what extent are behaviours and risks culturally defined?
- How do children's and adults' perspectives on risk differ?
- Which children's rights need to be protected?
- What behaviours need to change, and how can that change be achieved?

(b) The actions taken to date to strengthen children's right to protection at the international and national levels by governments, international agencies, the private sector and other key actors including legislation, law enforcement, policy developments, social welfare provision and international collaboration.

(c) Illustrative examples of protection-related initiatives on the ground. The report does not evaluate these initiatives and, while many look very promising, it does not propose them as proven good practice. Nevertheless, many examples cited are thought-provoking and merit further attention and follow-up.

In 2010, four initial background papers were developed for IRC and provided the basis for this publication. The papers addressed the following:

(a) Existing legal systems that govern cyberspace, in particular, those that protect children from abuse and exploitation in the online environment;

(b) Law enforcement policy and practice, and application of child-centred approaches in preventing and responding to sexual abuse and exploitation of children in the merged online/offline environment;

(c) The behaviour and activities of children and young people online, and the risks and potential for merged online/offline abuse and exploitation, including an overview of children's views and recommendations regarding risk-taking behaviour and preventive practices;

(d) Referral systems and rehabilitation services designed to respond to sexual abuse and exploitation of children in the merged online/offline environment.

The methodology did not involve primary research, but used secondary research that brought together the widest possible existing evidence from a broad range of countries. Given that academic research was not available from countries in every region, some use was also made of non-academic sources such as newspaper articles, press releases and non-governmental organization (NGO) reports to reflect, as far as possible, developments across all parts of the world. Evidence included:

- Data on the penetration and degree of usage of the Internet and mobile phones;
- Research evidence on patterns of behaviour of children and young people in the online environment;
- Research findings on the implications and impact of that behaviour;
- Research evidence on children and young people’s perspectives on their behaviour and its impact and implications;
- Findings from a survey on children’s experiences online, which was posted on the UNICEF Voices of Youth website for three months in 2010 and attracted nearly 1,000 responses;
- Evidence submitted to the Third World Congress against Sexual Exploitation of Children and Adolescents in 2008;
Earlier research on sexual abuse and exploitation from UNICEF IRC;

Review of recent reports from the Council of Europe, the European Union and the Organisation for Economic Co-operation and Development (OECD) on sexual abuse and exploitation of children online;

Review of international legislation relating to sexual abuse and exploitation and cybercrime;

Review of current law enforcement and social welfare challenges in the field of cyberspace and child protection;

Case studies submitted from countries representing different regions of the world, elaborating recent legal developments in protecting children and young people in the merged online/offline environment (countries were selected because their legal responses to harm against children in a merged online/offline environment offer insights that may be informative for other jurisdictions);

Case studies developed by the CEOP Centre, amplifying examples of how specific countries employed their law enforcement agencies to protect children;

Discussions with key experts in the field of law, law enforcement, social welfare and child protection (the social welfare material, for example, drew on responses from experts in Australia, Canada, the Czech Republic, Denmark, Egypt, Estonia, Finland, Germany, Iceland, India, Italy, Japan, Latvia, Lithuania, Malta, New Zealand, Poland, the Russian Federation, Serbia, Slovenia, Sweden, Taiwan Province of China, Ukraine, the United Kingdom, the United States of America and countries in the Caribbean);

Questionnaires on child protection in the online environment were sent to experts from a broad range of countries across the world, of which responses were received from 10 countries.6

The work was supported by an Expert Advisory Group that provided written comments on drafts and participated in a June 2010 consultative meeting in Florence, Italy, to review and discuss the background papers. This group reflected a broad range of professional expertise from all regions.

A considerable number of constraints in undertaking the study were encountered, resulting in limitations to both the scope of the findings and their reliability as a basis for programming in respect of all children. They include the following:

(a) The predominant body of available research derives from countries in Europe and the United States. While valuable, there are dangers in drawing generalized conclusions from evidence based on experiences in the most economically advanced countries. Although some research is being conducted in a number of other regions, it is less accessible internationally and often not published in English, rendering it inaccessible to the writers of this report.

Efforts were made to seek out as much information as possible from all regions, but the final paper is necessarily reliant, in terms of evidence, on a disproportionate body of data from the industrialized world. Some low- and middle-income countries – including Brazil, Egypt, Nepal, the Philippines and South Africa – have undertaken research in this area. These countries are heavily cited, not because they can be seen as representative of their regions or have any particular significance in terms of online behaviour, but simply because they have produced valuable research.

Apart from South Africa, there is a dearth of information from sub-Saharan Africa, and there is little in general from the Middle East and North Africa on children and young people’s patterns of online activity and potential exposure to risk. Nevertheless, the limited available research indicates some similarities, adjusted for cultural and social context, in usage of electronic media by young people.

(b) Each source study uses different data sets, methodologies and sample sizes; therefore, compatibility between sources is problematic. Similarly, different studies use different age ranges and definitions for children, young people and youth. Many of them, such as the International Telecommunication Union (ITU), include children aged 15–17 as part of the wider ‘youth’ category, which may run up to
In other studies. From a protection perspective, aggregating young people under age 18 with those over 18 makes it difficult to link statistical information with the legal implications of the Convention of the Rights of the Child and of many national laws.

(c) Existing research tends to focus on risk factors that children face. To date, there is relatively little evidence on the resilience and agency of children in managing the online/offline environment, or the strategies they adopt to protect themselves or mitigate risk. Some anecdotal information exists, for example, as to how children and young people are using mobile phones to alert others to danger, report abuse and support peers at risk, but these patterns of activity have yet to be adequately documented and researched.

(d) Differences in socio-cultural values and norms may affect research findings. For example, attitudes towards pornography within a society as well as how pornography is defined may determine whether a young person is willing to acknowledge that he or she actively sought out pornographic sites. Where doing so is seen as promoting status and machismo, for instance, boys might be happy to report using such sites. In other environments, they are more likely to describe their contact with such material as inadvertent or mistaken.

(e) There are groups of children about whose online activity and its implications are little known and for whom the experience may vary significantly from that of the majority—for example, children with disabilities; gay, lesbian, bisexual and transgender young people; or children without parental support.

(f) Rapid changes in the online environment and how children and young people use it and adapt to it cause research to become quickly outdated. It is a constant challenge to remain on top of the issue.

While taking these limitations into account, this report nevertheless provides a relatively comprehensive overview of the available evidence and a sufficiently robust analysis to point the way towards strategies for strengthening child protection in the merged online/offline environment.
PART ONE:

CHILD PROTECTION IN THE ONLINE/OFFLINE ENVIRONMENT

KEY MESSAGE

Information and communication technology is central to the lives of children and young people in industrialized countries and, increasingly, in the developing world. It is a key educational resource, providing information, entertainment, music and films. ICT is viewed by many as a fundamental part of their social lives. For children, the boundaries between the online and offline worlds have become seamless.

During the past decade, the world has witnessed an extraordinary change in the opportunities and means through which individuals and communities communicate with each other. The benefits of these developments are huge as the growth of electronic and digital media has afforded millions of people the chance to learn, publish and communicate on an unprecedented scale. Information and communication technologies offer opportunities for global exploration, dynamic interactive experiences and wide-ranging social networks. Initially, the fastest rate of penetration, or adoption and use, took place in industrialized countries, but today most regions of the world are rapidly catching up, particularly with the rise in mobile phone usage that enables access without reliance on fixed telephone lines.

Children and young people have a significant role in these developments. They tend to be early adopters of new forms of communication, a factor that has particular significance in the developing world, where the population under age 18 makes up a much higher proportion of the total compared to industrialized countries. Children and young people are not merely passive users of communication technologies; they are actively involved in creating and shaping them to meet their own demands and interests.

Young people are growing up in a world where electronic communication is increasingly considered to be as normal as face-to-face and telephone contact were for earlier generations. Whereas older adults conceptualize a clear distinction between the online and offline worlds, for young people building social networks in both worlds the differentiation is less meaningful. In this sense, the relationship between the virtual and physical worlds is becoming seamless or merged. Electronic media are central to the lives of an ever-growing proportion of children and young people in terms of social relationships and communication. They provide access to information, entertainment, games, the arts and culture as well as a way to create and exchange content.

Activities that previously took place only in the physical world are happening more and more online, and their nature and scope are being transformed. Through websites, blogs, social networking sites, mobile phones, microblogging platforms, chatlines, gaming sites, consoles and digital cameras, children and young people are expanding the scale of access to their peers and redefining the concept of friendship. These new media offer opportunities for young people to construct their lives in different forms from previous
generations. They can forge new, alternative and short-term identities, establish intense and constant levels of social engagement, build wide social networks and enter communities previously inaccessible to them.

Not only are the electronic and physical worlds of children and young people progressively merging, but their behaviours within cyberspace are affecting their experiences and activities as well as their risks and vulnerabilities across their day-to-day lives offline. This phenomenon is described in this paper as ‘the merged online/offline environment’.

Chapter 1: Understanding the social and cultural context

Locating children’s vulnerability to online-related sexual abuse and exploitation in a wider social and cultural context can provide a better understanding of the nature of concerns and how they are framed. Clearly, the context in which children are beginning to engage in the online environment varies hugely across and within different regions: there is no single global experience. There are some widespread patterns, however, which can be identified to help inform both how children’s behaviour online and adults’ reactions to their behaviour are related to day-to-day realities of the offline world.

First, as described, the world many children and young people now inhabit incorporates a virtual reality that was unknown to previous generations. For many children in the 21st century, their ideas, values, culture, aspirations and expectations of material goods are increasingly informed not by their parents or community and religious leaders but rather by the broader world around them, the pressures of commerce, advertising, and mass media, including the Internet. This experience of intergenerational divergence is far from new. But the scale and speed at which change is happening, to varying degrees of intensity depending on countries’ socio-economic and technological development, is of a different order.

Margaret Mead’s analysis of cultural forms is relevant in conceptualizing this change. Mead identified three divisions of culture: post-figurative, where knowledge and traditions are passed down from older to younger generations; co-figurative, where people learn from their peers; and pre-figurative, where rapid social change requires the younger generation to instruct their elders in how to function in a new cultural environment. Although all three forms can coexist, the advent of new forms of social media, the speed of their penetration into cultural life, their growing predominance in children and young people’s lives, and the consequent changes required in skills, practices and patterns of behaviour mean that children and young people are more often transmitting their knowledge to the older generation rather than the other way around.

As noted by Tanya Byron, “The trouble is that although as adults we instinctively know how to protect our children offline, we often assume that their greater technological expertise will ensure they can look after themselves online. But knowledge is not the same as wisdom.”

KEY MESSAGE

Through ICT, young people are exposed to information, values, ideas and opportunities beyond those of their families or religious or community leaders, using a medium that many adults do not understand or access in the same way. Such exposure has the potential to transform aspirations and behaviours. However, unless parents are also directly engaged with ICT or effectively communicate with their children about their online experiences, their capacity to understand their children’s experiences or offer effective protection is limited.

In the Internet age, a growing number of contemporary societies could be described, in one sense at least, as being in a pre-figurative pattern of cultural development. Growing numbers of children are now creating and exploring their own virtual social networks. Through exposure to knowledge, information, online advertising, and political, religious, cultural or sexual ideas that may be profoundly at odds with those of their parents, children’s and young people’s worlds are significantly more complex than they have been hitherto.
Therefore, there are also concerns that greater access and exposure to electronic media can have harmful implications, including potentially diminishing parents’ capacity to provide a protective environment for their children.11

Second, in much of the industrialized world, there has been an emerging fear of the unknown paedophile, an adult who is sexually attracted to children, as an ever-present threat. Media exposure in many countries during the early 1990s intensified and fed this fear. In the United Kingdom, concern about such perpetrators of sexual abuse became widespread following exposure of child sexual abuse in residential childcare homes and other institutions where children were supposed to be protected.12 A high-profile case that hit the headlines in 1996 was that of a released sexual abuser charged with a series of child murders in Belgium.13 Meanwhile, also in 1996, ‘Megan’s Law’ was created in the United States following the rape and murder two years earlier of a 7-year-old girl by a twice-convicted sex offender who lived on the same street.14

**KEY MESSAGE**

*There is a risk of ‘moral panic’ concerning the Internet. Although the Internet does provide a new avenue for child abuse, it is important that is weighed against the many benefits it provides for children.*

Although these cases undoubtedly represent grave criminal offences against children, the sensational media coverage led to a perception of a growing threat to children, despite evidence that such risks are both rare and not increasing.15 The Internet has exacerbated these fears, providing a new environment where children, particularly girls, are seen to be at ever-growing risk.

The fact is that prevalence rates of child sexual abuse are quite high, but in general, perpetrators are known by and close to the children they abuse. In the United States, the percentage of single offender crimes against girls where the offender is an adult and a stranger has declined since 1994, concurrent with the rise of Internet use. According to the Juvenile Offenders and Victims: 2006 National Report, the 2003 non-fatal, violent victimization rate of 12- to 17-year-olds was half that of 10 years earlier. Overall, the rate of serious violent crimes against children aged 12–17, including aggravated assault, rape, robbery and homicide, was on the decline for both boys and girls.16

‘Moral panics’ in respect to emerging technologies are not a new phenomenon. There were many fears about the use of the telegraph in the 1800s, with disapproval of women using it for communication.17 Women were considered to be naive and incapable, and a virtuous woman was supposed to be technologically ignorant. In the early 20th century, the telephone was considered to be a method by which illicit conversations could happen and sparked panic that it would encourage girls to be more aggressive in their approach to men and would threaten parental control.18

Caution is therefore necessary in response to concerns about risk in the merged online/offline environment. Obviously, children are exposed to additional risks in this new social space but the popular fear that the Internet endangers all children has not been supported by the research evidence so far.19 The crucial issues that need to be addressed are the scale of the problem, the nature of the risk, and which children are vulnerable and why.

Third, the period in which cybertechnology has become so dominant in the lives of children coincides with a period, predominantly in industrialized countries, where anxieties about paedophilia (together with crime and safety in general) have led to severe restrictions in the social freedoms associated with childhood. Children, particularly middle-class children, are far less likely to be allowed outside to play independently and increasingly have their social lives and entertainment managed by parents. This pattern is well established in many industrialized countries and is also becoming the case among the middle class in middle- and low-income countries.20 Parents’ increasing containment of children has been accompanied by mounting adult perceptions reinforced by politicians and the media that public space is the legitimate sphere of adults and that children in public space are at risk, a nuisance or a threat.21

The physical world is far less accessible to many contemporary children in industrialized countries than it might have been to previous generations.22 There are restrictions in other parts of the world too, such as the Middle East, where public spaces are highly regulated for young people, particularly girls.23 The process
of denying children access to the public sphere influences the way they shape their identities and learn social skills.24

**KEY MESSAGE**

In high-income countries, anxiety about risks of harm from paedophiles and other threats has led to growing restrictions being placed on children. It is important to keep in mind, however, that while children need protection, the Internet also provides them with a new and exciting route for interaction and exploration.

The desire to protect children from the external environment is challenged by the rise of the Internet, with its rapidly expanding opportunities for communication and networking, and as a substitute for or complement to the street or the playground. As Yvonne Jewkes, criminology professor at the University of Leicester, observes: “Adventure is, for many children, a virtual pleasure; competitiveness is honed at the games console rather than on the sports field; and sexual development occurs in chat rooms, on social networking sites and via mobile phones.”25 As children in some parts of the world are subjected to continuing or increasing controls over their physical autonomy, they are discovering a virtual world in which to explore, interact and play. The Internet offers a young person the opportunity to engage in an infinite world of connections and contacts while sitting at home in their room. It therefore requires a rethinking of how to effectively protect children.

The irony is that this virtual world offers a degree of freedom of expression, including sexual expression, and of thought. It offers the opportunity to construct an identity and access information far beyond that to which children and young people have in the physical world and in ways in which their parents are far less equipped to intervene. Young users of social networking sites, for example, perceive these areas as private and free from parental control while allowing opportunities for regular and instant communication with their peers.26 This pattern is not just exemplified in industrialized countries. In at least one Middle Eastern country, unrelated male and female teenagers, who are prohibited by authorities from talking to each other, let alone meeting, are beginning to subvert controls on their behaviour by using Bluetooth technology (allowing electronic devices to transmit wirelessly) to share images and communicate with each other without risk of being caught.27

Fourth, in a growing number of countries, the messages children receive from an early age concerning sex and sexuality are contradictory. In Australia, North America and many European countries, growing fears over sexual abusers have led not only to children being subject to increasing protection, but also to a fear of all adults who might have close contact with children. In some places, there are reports of primary schoolteachers not allowed to touch any child in their classes, and there is general suspicion of any adult who approaches or speaks to a child.28

Fear about children’s exposure to sexual assault in the real world and via the Internet coincides in the industrialized world with anxieties about the increasing sexualisation of the social environment and of children themselves. Examples commonly cited include makeup for children, fashion collections themed around Lolita, sexualized music videos on weekend morning television, sexually explicit ‘adult only’ DVD covers in local video shops, sexually overt and often degrading lyrics in popular songs, highly sexualized dolls, padded bras for pre-teens and explicit billboards.29 Some researchers, such as Linda Papadopoulos in a review for the UK Home Office published in 2010, argue that the constant bombardment with sexual imagery has shifted the boundaries of behaviour and expectation deemed acceptable for children, especially girls, in ways that are harmful.30 Not all researchers agree on the impact on young people, but the views of Papadopoulos and others are at the very least indicative of a strong groundswell of concern in the wider public.31

Fifth, attitudes towards sexual exploitation and abuse of women and girls within any given culture also influence behaviours in both the online and offline environments. If a society tolerates sexual violence against women and girls offline, for example, it is unlikely that behaviours involving online communication or interaction will be very different.
Sixth, children are not empty or passive vessels. They play an active role in interpreting and constructing the world around them. But in doing so, they are influenced by age, gender, family environment and culture. Adolescents are at a stage of life when they are likely to explore and experiment, including with their sexuality, while pulling away from adults to define their own place in the world.

Although many of the developments described here reflect phenomena observed largely in industrialized countries, they serve to illustrate how a complex interplay of social and cultural phenomena influences how children understand the world in which they are engaged – its moral and ethical boundaries, the nature of risk, expectations and normality in sexual behaviour. These phenomena provide the lens through which adults in general and parents in particular construct their relationships with children and the way in which adults understand risk. They impose limits on the degree of adult access to the worlds that children inhabit.

It is important to recognize that children’s activities and the challenges they face do not occur in a social vacuum. To influence and minimize children’s risk of abuse and exploitation, adults need to understand the context and complexity of their lives.

Chapter 2: Sexual exploitation and abuse in the online/offline environment

The rise of the online environment has not created crimes of sexual abuse and exploitation of children. But new venues for content, contact or conduct online do allow much easier access to a wide range of children, increasing the scale of ‘opportunity’ and the potential for causing harm. Images of children are easier to create and distribute, viewers can easily turn into exchangers, and traders and producers of child abuse materials can open new arenas for distribution of their ‘products’. The Internet environment has allowed children themselves to initiate and engage in sexually explicit behaviours with an apparent degree of anonymity, and adults who seek to perpetrate online or offline sexual exploitation and abuse to make contact with children and young people.

Children and young people vulnerable to abuse and exploitation can fall into three broad clusters:

- Younger children who are sexually abused and photographed, by or with their parents or caregivers collusion, for the purposes of online exploitation;
- Older children who place sexualized images of themselves online, and in doing so, expose themselves to potential grooming and exploitation;
- Young people who are the victims of their peers, who may assault them, photograph them and distribute the images online.

Risks, however, should be viewed in a broader context. For the vast majority of children and young people, their online behaviour does not lead to victimization or harm. Behaviours that have the potential to place them at risk are dealt with in subsequent chapters. To understand the context in which those risks arise, it is necessary to review the available research on the scale of online sexual abuse and exploitation, the forms they take, the children who are abused online, and the nature and numbers of online abusers.

Child abuse images

Sexual abuse and exploitation of children through images spans material that is suggestive to images depicting explicit sexual activity. Although most international and much national legislation refer to these images as child pornography, there is increasing preference among law enforcement and child protection agencies for the term ‘child abuse images’, which places a stronger emphasis on,
and recognition of, the abuse and exploitation of children perpetrated through such images.

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. The IWF acknowledges the difficulty in comparing data from different years due to the rapid changes in hosting arrangements of child abuse images, which render the numbers of images and web pages to be no longer comparable. The increase could be attributed to a change in hosting patterns; instead of posting collections of images in a folder on a single web page, content is being posted on separate websites. 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).

There are millions of child abuse images on the Internet, with tens of thousands of individual children depicted in the images. In April 2010, the National Society for the Prevention of Cruelty to Children (NSPCC), one of the leading child protection charities in the United Kingdom, published a study in which media reports of court cases in England and Wales between April and September 2010 were analysed. The NSPCC found that close to 3 million images had been circulated by 284 offenders who were consequently convicted. Some 35,000 images were classed as categories 4 and 5, which are the most severe levels of abusive images as set in the guidelines issued by the Sentencing Guidelines Council Advisory Panel (England and Wales) in 2002.

Once on the Internet, images can easily be transmitted to other websites, downloaded onto mobile phones or prepaid cards that reduce traceability have all contributed to the potential for online abusive and exploitative activity towards children.

Perpetrators can also sell children for live abuse online, in which the perpetrators announce to their online ‘peer’ or ‘peer group’ their intention to abuse a child on a set date and time. Those who wish to watch the live abuse arrange with the perpetrator to be online at that time. Payment may be in money or through bartering, such as exchanging images or drugs. Children may be lured into the perpetrator’s house and sexually abused, and may or may not be aware that live transmission is occurring.

Recent evidence from the European Financial Coalition against Commercial Sexual Exploitation of Children Online indicates that organizers of commercial child abuse websites distribute images but do not produce them. Not all distributors are from organized criminal networks; many are individuals working together who may or may not have a personal sexual interest in children. Once posted, the images are difficult to retrieve. The child has no control over his or her images, and these images can remain in cyberspace in perpetuity. Some current images may have been produced more than 20 or 30 years ago and have since been digitized and posted online.

The vast majority of images in cyberspace, however, have been produced much more recently and are linked to the emergence of cheap, easy-to-use, high-quality digital cameras and to the development of the Internet as a mass consumer product. These newer images may derive from within the child’s family or social circle or be procured through child prostitution.

The public posting of child abuse images online can have lasting consequences for children. Since the images are almost impossible to erase once in cyberspace, the children in these photos may realize that for the rest of their lives someone could be looking at their pictures on the Internet. The threat of publication alone may be a form of coercion used by child sexual abusers, allowing them to continue long-term abuse.

The children in child abuse images

A significant proportion of child abuse images online are of young children, with an identifiable downward trend in age. According to the IWF 2010 Annual Report, 73 per cent of the child victims identified in online child sex abuse...
images appear to be less than 10 years old. Other analyses of online images confirm the preponderance of prepubescent children. There is also evidence that the images are becoming more graphic and more violent. The IWF, for example, found that sexual activity, including rape and torture, between adults and children was depicted in more than 65 per cent of still images and videos found online.

Girls and Caucasian children also figure disproportionately. Studies from Australia, New Zealand, South Africa and the United Kingdom have consistently found that the child sexual abuse images on the Internet are of mostly Caucasian, westernized, female children, 8 to 12 years old. In much of the research, the main context for the abuse appears to be domestic, and the relationships between those producing the images and the children are familial or of social proximity.

Ethel Quayle and Terry Jones recently carried out the first systematic study of a random sample of abusive and sexualized images of children distributed through the Internet and obtained through a police database of seized collections. They found that the odds of children in the abuse images being female versus male were about 4 to 1 and the odds of the images being of Caucasian children versus non-white children were about 10 to 1. Compared with female children, male children were more likely to be prepubescent or very young. Compared to white children, non-white children were more likely to be prepubescent but less likely to be very young.

**KEY MESSAGE**

Child abuse images tend to feature children aged between 0 and 10 years old, Caucasian and female. Those who become the victims of grooming tend to be adolescents.

These results are similar to those found across all other samples taken from seized collections of images, reported content of web pages and identified children. With regard to the issue of ethnicity, the preponderance of Caucasian children in sexualized images could 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.

When developing protective strategies, it is important to differentiate between those children who are being forced into sexual exploitation and abuse, either through their parents or other adults in their lives, and those whose personal online activities and behaviour may under some circumstances place them at or expose them to risk. Given the disproportionate numbers of very young children represented in the child abuse images worldwide, it appears likely that exploitation by family members is involved in a significant number of cases.

**Grooming**

Grooming has been defined as the process of ‘befriending’ a young person online “to facilitate online sexual contact and/or a physical meeting with them with the goal of committing sexual abuse.” Cyberspace provides a variety of forums in which predators can groom their potential victims through chat rooms, social networking sites and instant messaging. Offenders use online networks to communicate with each other and show live-time abuse and share images to gain credibility among other offenders, and research in the United States suggests that arrests for Internet sex crimes against children often have a social networking site connection.

The European Online Grooming Project reports that evidence from stakeholders indicates that offenders may have up to 200 young people listed as online ‘friends’ at various stages of the grooming process, and that they typically use the ‘success’ of previous contacts with young people as a basis for adapting their activities. These processes of online grooming may take minutes, hours, days or months, depending on the goals and needs of the abuser and the reactions of the young person. Offenders can move from online grooming towards an offline sexual assault. Alternatively, the relationship may be pursued by persuading the child to send sexually explicit images of herself or himself, which are then used and disseminated to networks of sexual abusers.

Offenders use online networks to communicate with each other and show live-time abuse and share images to gain credibility among other abusers. There is also evidence of an increased use of webcams linked to instant messaging,
employed to coerce a child into witnessing or performing sexual acts.\textsuperscript{55}

Who is vulnerable to being groomed is discussed fully in a subsequent section. In terms of age, evidence suggests that adolescents are most at risk, particularly adolescent girls. At that stage, young people 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 and their sexual and emotional identities.

### Abusers and exploiters online

Many forms of behaviour constitute child sexual abuse. The range may include adults who sexually exploit their own or others’ children for the production of images; who download images for their own personal use; who exploit children by creating and distributing images, but not necessarily for their own use; and who seek children online in order to abuse them.

### Numbers of offenders

The number of people who offend via electronic media is unknown. Most of the data currently available relate to the production, distribution and viewing of child abuse images. Although conviction rates provide some indicators, they reflect only the countries with relevant legislation regarding possession and distribution of abusive images and online grooming, and with the resources and resolve to investigate and prosecute such acts.\textsuperscript{56}

Recent data from authorities in Norway, a country with a population of less than 5 million, where access to known sites with child abuse images is blocked, reveal that there are as many as 15,000–18,000 daily attempts to access such images; however, this does not represent 18,000 different individuals.\textsuperscript{57} These figures need to be interpreted with a degree of caution since, for example, they include ‘hits’ that come from web crawling robots, which are generated by an automated process rather than an individual ‘visitor’. They nevertheless indicate the scale of interest in and viewing of child abuse images.

There is no information on the number of individuals who are grooming children online. In many countries, such activity is not a crime and no records exist relating to such behaviour. Even among those countries where it has been criminalized, there are no coordinated databases of offenders.

### Demographics of offenders

Regarding the characteristics of those who create, view and distribute child abuse images, there are striking demographic consistencies found in studies undertaken during the past 5–10 years. Janis Wolak, David Finkelhor and Kimberly Mitchell, for instance, found in their 2003 and 2005 studies of sexual Internet crimes against minors that 99 per cent of their sample was male,\textsuperscript{58} and similar patterns have been seen in later research.\textsuperscript{59} More recently, examples have surfaced of women being implicated in the online/offline sexual abuse of children. In 2009, several women in the United Kingdom were discovered to be abusing young children offline, photographing the abuse and then distributing the images online to a ‘male friend’.\textsuperscript{60} During 2010, 23 people in Sweden were arrested for exchanging abusive images of children; 20 of them were women, 40 to 60 years old, who met on an Internet dating site, according to the media and a police spokesperson.\textsuperscript{61}

The Internet makes the development of offender networks easier, which in turn can exacerbate abuse by providing incentives for producing more extreme images. CEOP has observed more offenders meeting online via Facebook and other social networking sites. Joining a network also allows novice offenders to overcome inhibitions and develop offending behaviour among like-minded individuals.\textsuperscript{62}

The limited research data available to date indicate that the majority of known offenders are Caucasian and Western.\textsuperscript{63} One analysis of offenders in the United Kingdom found that Internet-related offenders were predominantly Caucasian compared with the broader offence of child molestation, which was committed by persons from a wider range of ethnic groups.\textsuperscript{64} Some 86 per cent of Australian Internet sex offenders were identified as Caucasian, with Asian, Mediterranean and Aboriginal ethnic groups minimally represented.\textsuperscript{65} It is not clear, however, whether these offender characteristics are a result of socio-demographic patterns of Internet use, and therefore may change as use begins to extend more broadly into all sections
of society, or whether they reflect differences associated with cultural patterns of behaviour.

**KEY MESSAGE**

Perpetrators of online abuse are not restricted to the popular image of the ‘paedophile as pervert’. Significant numbers of (mostly) men download child abuse images on a regular basis. The available evidence indicates that the vast majority of perpetrators are male, Caucasian, employed, reasonably well-educated and span a wide age range.

The available evidence on offenders’ ages provides a more varied picture. Research in the United States in 2005 indicates that 45 per cent of individuals arrested who possessed child abuse images were aged 40 or older, and this is similar to other more recent reported findings (in Australia, for example). However, data gathered in 2005 by the New Zealand Censorship Compliance Unit found a significant level of offending behaviour among younger men. Of the 201 cases in its 2005 analysis, the largest single age group was 15 to 19 years old, which accounted for just over 24 per cent. More than half were under 30 at the time of the investigation. However, subsequent updates (2007 and 2009) have shown an increase in the mean age of offenders. A United Kingdom analysis of 100 convictions from September 2008 to March 2010 for possessing, making and distributing child abuse images found that the number of offenders was relatively evenly distributed across the age range of 20 to 59, with the number of convictions decreasing among offenders aged 60 and older.

It is difficult to determine the extent to which children are engaged as perpetrators of online abuse. Criminal statistics refer only to offenders over the age of criminal responsibility and cover only reported offences, but much abuse goes unreported or is not recognized and dealt with as such. Various studies have tried to estimate the extent of sexual abuse by children. In terms of sexual abuse offline, previous evidence from the United Kingdom and United States indicates that 20 to 30 per cent of abuse in those countries is perpetrated by children, mainly during adolescence.

The research also points to relatively high levels of education and professional status among abusers. In the New Zealand sample cited above, students were the largest group; two thirds were studying at the tertiary level, of which around 38 per cent were studying subjects related to information technology. In the Australian research, the offender was typically a professional or in an administrative role, was minimally competent on a computer, and did not employ sophisticated technology or security measures.

Research conducted in the United States in 2005 indicates that 73 per cent of the sample population was in full-time employment, with 82 per cent having an income greater than $20,000. Similarly, in a 2007 study conducted in the United Kingdom, just more than half had received tertiary education and some 75 per cent were in a full-time occupation; unlike the New Zealand group, this study indicated that nearly 93 per cent had not received any formal training in Internet use. An NSPCC survey of court cases in the United Kingdom found that one in four held positions of trust, including teachers, clergy, medical personnel and police officers.

Overall, the picture that emerges is that those who view child abuse images online are typically male, white, reasonably well-educated and employed, and span a wide age range, including young people. Certainly, the evidence does not reflect the stereotype widely portrayed in the media. Public perceptions of paedophiles as socially marginal sexual predators may blunt the reality of the sexualization of children, particularly girls, in various cultures and the prevalence of sexual abuse and exploitation among the general population.

**Links between online and offline abuse**

The available evidence on the link between online and offline abuse is somewhat contradictory. A study published in 2005 in the United States found that 40 per cent of people arrested for possessing child abuse images were ‘dual offenders’ who had sexually victimized children and possessed child abuse images, suggesting there may be a correlation.
Research undertaken in the United States and published in 2008 based on a review of official records and self-reports made by 155 imprisoned child pornography offenders enrolled in an intensive residential treatment programme, found considerable similarities between those who had a documented history of hands-on sexual abuse (26 per cent) and those who did not (74 per cent). Both types of offenders had previously undetected contact sexual offences, and 85 per cent of all the offenders in the programme admitted to having at least one offline sexual contact with a child. In total, they victimized 1,777 children – an average of 14 victims per offender. The vast majority of offenders reported that they committed offline abuse prior to seeking child abuse images via the Internet, suggesting that the online environment may provide an additional outlet for criminal behaviour. The findings in this research are consistent with evidence from the United Kingdom, which indicates that offenders frequently switch between the Internet and the offline environment in order to target young victims, with the ‘virtual’ environment providing potential opportunities for extending existing offending behaviour.

However, other research on individuals who possess child abuse images differs in that a significant majority has never been associated with or prosecuted for contact crimes of sexual abuse. This leads to the question of whether the Internet is creating a new form of sexual offender, one that views abusive images of children but does not go on to sexually abuse a child offline. A recent study by David Middleton suggests that, in relation to offenders serving sentences for viewing child abuse images, there is “a population of Internet offenders who do not share the psychological vulnerabilities typically displayed by sex offenders.”

Another study, published in 2010, explored the Internet sexual activity of two groups of adult male ‘child pornography offenders’ (contact and non-contact child pornography offenders) and sought to identify potential risk factors associated with those offenders who also sexually abused children. It concluded that possessing child abuse images is not of itself a causative factor in the perpetration of offline child sexual abuse and that other factors need to be considered when evaluating the level of danger these offenders present, and when planning their treatment and supervision in the community.

This evidence points to a cohort of ‘child pornography’ offenders who appear not to seek to make contact with children offline. While the Internet has created new opportunities for them to express their sexual interest in children, without that ‘expression’ they would not have become known to the criminal justice system. Nevertheless, there is need for caution in assessing potential risk. Offenders who have accessed child abuse images online have demonstrated a sexual interest in children and may therefore eventually seek contact with them even if they have not yet done so.

Child abuse images legitimize contact child abuse: children are sexualized; masturbation to sexualized images of children and child sexual abuse reinforces the association between children and sexual gratification; child sexual abuse images normalize the notion of sex with children; and images suggest types of sexual abuse to the viewer.

Images therefore provide the motivation for contact sexual abuse and facilitate the overcoming of inhibitors to commit it. At the very least, such offenders have contributed to sustaining demand for the production of images that involve the physical sexual abuse of children by others.

Many individuals downloading child abuse images were previously seen as responsible members of their communities. A starting point, therefore, in seeking to protect children from sexual abuse must be to recognize that it is perpetrated by a wide range of adults and children, often opportunistically. This awareness needs to inform any strategic investment in developing more protective environments for children.

Chapter 3: Children’s activities using information and communication technology

To better understand children’s and young people’s activities and behaviours online, and the extent to which they place them at risk, it is
important to appreciate the degree of access to the Internet and other new media in children’s lives and the varying ways they are used across different parts of the world. In recent years, for example, the opportunities for communication have expanded from email and websites to social networking sites, mobile phones, blogs, chatlines, gaming and digital cameras. These modes of communication influence the speed and frequency of access as well as the nature of children’s interactions. Although the developing world is rapidly catching up, there remains wide variation in access to electronic media as well as in how and where it is accessed.

Given the speed of change in this field, available data on the rates of Internet and mobile phone usage are likely to be outdated quickly. This is particularly true with the emergence of smartphones, which increasing numbers of young people use to access the Internet. A review of the main studies available, however, reveals valuable information on emerging patterns.

Levels of Internet access and usage

A high percentage of children in the industrialized world have Internet access. An ITU statistical compilation published in 2008 found that, with few exceptions, children and youth are more likely to use computers and the Internet than the general population. In 2006, 65 per cent of children aged 10 to 14 and 90 per cent of young people aged 15 to 19 were going online in Japan. A 2009 survey conducted in schools and on the Internet of 4,338 boys and girls aged 14 to 17 from 17 regions across the Russian Federation found that nearly all schoolchildren had access to the Internet. More than 50 per cent of students spent several hours on the Internet each time they accessed it.

In the United States, a survey of 800 adolescents aged 12 to 17, conducted in 2009, found that Internet access is almost universal, with 93 per cent going online. During the past 10 years, teenagers and young adults have been consistently the two groups most likely to go online. Across Europe in 2009, 75 per cent of children between 6 and 17 years of age (85% of children between 11 and 17) used the Internet, although there were wide variations between countries. The highest levels of access were in Northern European countries, where it was generally more than 90 per cent, compared to Cyprus and Greece, at 50 per cent.

This phenomenon has moved beyond the industrialized world as Internet access is increasing globally. Children’s and young people’s online access has mushroomed in some countries, but the degree and forms of access vary across regions and are usually different within countries according to socio-economic background. In Brazil, for example, the number of people aged 10 and older who logged onto the Internet between 2006 and 2009 increased by more than 75 per cent, to 56 million users. 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.

A study of 10,000 girls and young women aged 14 to 21, living in 10 cities across India, found that more than two fifths of them were aware of the Internet. Awareness varied significantly across the cities, however, with only 10 per cent aware in Patna and Varanasi, compared with more than 74 per cent in Hyderabad. The same study shows that only 4 per cent of the girls who lived or worked on the street knew about the Internet.

A 2009 survey in Nepal provided anonymous, self-administered questionnaires to 1,430 children aged 12 to 18, some from private and public schools and others out of school. It was complemented by focus groups in which 106 children participated. The study found that, on average, 82 per cent – 74 per cent of girls and 91 per cent of boys – used the Internet and tended to spend one to four hours per week online. Of those, 63 per cent were using Internet cafes, while 51 per cent also had access at home.

In sub-Saharan Africa, overall Internet penetration remains low, at just less than 11.5 per cent as of 30 June 2011, but the growth rate over the past decade has been extraordinary: more than 2,500 per cent. In South Africa, for example, less than 5 per cent of all households had a working connection in 2008, but the Internet was being accessed through cybercafes, mobile phones, at work and at school. In a study of 934 questionnaires completed by adolescents aged 13 to 17 living in South Africa’s urban areas, 52 per cent reported accessing the Internet at home, with 37 per cent...
also having access at school and 23 per cent at public venues.\(^{95}\)

Although there are regional and country differences, gender and Internet access have little correlation across the vast majority of the world. In 2009, EU Kids Online examined findings from countries in the European Union on children’s use of online technologies and identified limited variance in access and use between boys and girls.\(^{94}\) The 2008 ITU statistical review found that the number of boys and girls aged 5 to 14 who used the Internet was similar in both industrialized and developing countries for which data were available; the exception was the Occupied Palestinian Territory, where boys used the Internet twice as much as girls. In Azerbaijan, among youth aged 15 to 24, a significantly higher number of young men used the Internet compared to young women, whereas in Cyprus the trend was reversed.\(^{96}\) No analysis is available of why these patterns exist. A survey in South Africa found a slight gender difference, with 56 per cent of boys compared to 49 per cent of girls accessing the Internet.\(^{96}\)

Socio-economic factors, on the other hand, impact access significantly. This is seen in Europe, where social inequalities persist and 76 per cent of children of highly educated parents have Internet access, compared to 61 per cent of those from the lowest educational group.\(^{97}\) In the United States, white teenagers are somewhat more likely (39 per cent) to use the Internet several times a day than African American adolescents (33 per cent) or those from Latin America (26 per cent), possibly reflecting patterns of socio-economic differences.\(^{96}\)

Age is another factor that affects Internet access, and, generally, access increases along with a child’s age. But younger children are going online in greater numbers, and the age of first-time Internet use is declining. In the European Union, based on parental perceptions, an estimated 60 per cent of children aged 6 to 10 were using the Internet in 2008, compared to 86 per cent of those aged 15 to 17.\(^{98}\) Similarly, the 2008 ITU statistical report found that the 5 to 14 age group was far less likely to use the Internet at least once a day – and far more likely to have access less than once a week – than the population as a whole or young people aged 15 to 24. Hong Kong was the exception, with only a marginally lower number of 5- to 14-year-olds using the Internet regularly.\(^{99}\) The opposite pattern is found in South Africa, where 54 per cent of children aged 13 to 16 access the Internet, compared to 45 per cent of those older than 17.\(^{101}\) The study in India found that among young women aged 18 to 21 there was slightly higher access, at 18 per cent, compared to 13 per cent among girls aged 14 to 17.\(^{102}\)

**KEY MESSAGE**

Children’s use of the Internet, their behaviour online and their vulnerabilities within the online environment are different at different ages. Recognition of children’s evolving capacities is needed, with corresponding protection strategies that are appropriate to their age and level of understanding.

The 2011 EU Kids Online survey found that, across 25 countries, one third of 9- and 10-year-olds who use the Internet do so on a daily basis. The average age of first-time Internet use is 7 years old in Sweden and 8 years old in other Northern European countries.\(^{103}\) Another report reveals that the age of first use of the Internet among children in Sweden has dropped from 13 in 2000 to 4 years old in 2009; the report concludes that at least half of all 4-year-olds use the Internet at least occasionally.\(^{104}\) The ITU survey found that little data are available for children aged 5 and under, with the exception of the Republic of Korea and the United States. In the Republic of Korea in 2007, 34 per cent of 3-year-olds, 47 per cent of 4-year-olds and 69 per cent of 5-year-olds used the Internet, though it is hard to know how significant this is without knowing what is counted as an ‘Internet user’ and what the figures would be from other countries.\(^{105}\)

In addition to children and young people gaining more access to the Internet, they are also spending considerably more time online. The EU Kids Online study found that 93 per cent of 9- to 16-year-olds go online at least once a week and 60 per cent do so every day or almost every day.\(^{106}\) In 2007, British children aged 12 to 15 spent an average of 13.8 hours per week on the Internet, nearly twice as much time as in 2005, when they were online for 7.1 hours per week.\(^{107}\) Further data on the pattern and extent of children’s access to the Internet were generated by a 2008 global online poll conducted by the International Youth Advisory Congress (IYAC) and coordinated by CEOP.\(^{108}\) The poll recorded the views of
1,277 children and young people, the majority of whom were 11 to 14 years old; 54.6 per cent were female (the poll respondents were overwhelmingly European, despite efforts to get global perspectives; specific countries from which children responded are not provided in the documentation). While the survey results indicate that respondents were using many different means for online access, just over 28 per cent reported using the Internet between one and two hours per day and nearly 21 per cent between two and three hours each day; nearly one quarter of respondents said they use the Internet from three to more than five hours per day.

A 2006 study in South Africa discovered that 48 per cent of high school students accessed the Internet less than once a week and 53 per cent spent less than an hour per week online. A study in Bahrain, on the other hand, determined a high level of Internet access, with young people using it on average two and a half to three and a half hours a day.

One of the most striking facts to come out of a 2009 survey by the ITU of 9,000 adult and child Internet users in 12 countries is the difference between the amount of time that parents believe their children are spending online and the amount of time children say they spend online. The survey found children were spending on average 39 hours per month on the Internet, twice as much time as their parents believe. As stated in the survey, “The Internet is kids’ new backyard.”

Where children and young people access the Internet varies. Most Internet access in the industrialized countries and advanced Asian economies is from home, whereas young people in the developing countries are more likely to access the Internet from school or Internet cafes. In the United States, 84 per cent of children have access to the Internet at home. In the European Union, 87 per cent of children aged 9 to 16 access the Internet at home, 63 per cent at school and 33 per cent via a mobile phone or handheld device.

Within the European Union, one of the biggest changes in recent years has been the level of parental access to the Internet. In 2008 an average of 84 per cent of parents throughout the region had used the Internet compared to 66 per cent in 2005. Far more children were online in 2005 than their parents, yet today this is no longer true. With few exceptions, use by children and parents is about the same. In Europe, only 9 of 27 countries surveyed had more children online than parents, and then only marginally.

Use of mobile phones

The explosion in mobile phone use is significant in two ways. The first is that communication with peers is of fundamental importance to many teenagers. The mobile phone provides an almost unlimited opportunity to remain in continuous contact, by text as much as by voice, and for this reason is now considered to be a necessary social tool for young people in many industrialized and middle-income countries. The second is that mobile phones are becoming more sophisticated and increasingly enable Internet access.

Globally, total mobile phone connections reached 4.98 billion in the second quarter of 2010, with the world’s population then standing at 6.8 billion. The number of active mobile subscriptions in Africa reached 506 million at the end of September 2010. Africa was one of the fastest growing regions in the world, with an 18 per cent increase of subscriptions between January and September 2010. Africa’s largest mobile market is Nigeria, which accounts for 16 per cent of African mobile subscriptions, followed by Egypt and South Africa. Of the 54 million new subscribers in Africa’s total mobile subscriptions during the first nine months of 2010, Egypt, Morocco, Nigeria, the United Republic of Tanzania and Zimbabwe accounted for 48 per cent. Best estimates suggest that the strongest growth rates in mobile subscriptions will occur in the East and Central African markets, including the Democratic Republic of the Congo, Eritrea, Ethiopia and Madagascar, with a projected increase of more than 100 per cent by 2015. These data are not disaggregated to provide a clear picture of the scale of child ownership or mobile phone use, but, undoubtedly, this growth is having an impact on children’s access to mobile phones.

A similar pattern of growth has taken place in South Asia. Data show that by March 2010, Bangladesh had 54.7 million mobile subscribers among a national population of 156 million. In India, the number of mobile subscriptions reached 508 million by the end of 2009. According to market estimates, the number of active mobile subscriptions in India will reach 1.16 billion by the end of 2013, which would make it the largest mobile market in the world.
The total number of mobile phone subscriptions in Latin America reached 580 million, according to information from March 2011. It should be noted, however, that this number includes mobile broadband subscriptions and the fact that people have more than one subscriber identity module (SIM) card. The largest and most important mobile market in South America is Brazil, with 206 million subscriptions and 105 per cent penetration by the end of December 2010.

Mobile phone ownership among children has also jumped during recent years. By 2008, on average more than two thirds of children across Europe aged 6 to 17 had a mobile phone, with the proportion increasing to 94 per cent among those aged 15 to 17. According to the Pew Internet & American Life Project, which tracks teen cellphone use, 45 per cent of children in the United States aged 12 to 17 owned a mobile phone in 2004; this figure rose to 71 per cent in 2008, including 52 per cent of children aged 12 to 13 and 84 per cent of 17-year-olds. Cellphone ownership among teenagers in the United States was found to be positively correlated with parental income; 62 per cent had a cellphone among those whose parental income was less than $30,000, increasing to 79 per cent where parental income is more than $75,000.

Moreover, the age at which children acquire their first mobile phone is dropping. The Pew Research Center’s Internet & American Life Project confirms this trend, finding that 18 per cent of children aged 12 owned a cellphone in 2004 and 58 per cent owned a device in 2009. A 2004 survey of around 90 children in the United Kingdom, aged 11 to 16, found that mobile phones are sometimes seen as a key feature in their maturation: ownership is a coming-of-age symbol.

Mobile phones can provide an illusion of protection for both parents and their children. The mobile phone facilitates a far higher degree of contact with children, enabling parents to communicate whenever the child is outside their reach, and can maintain a safety line in the event of danger or risk. Yet smartphones also offer children and young people virtually unlimited and unsupervised connection to the Internet. A survey of about 20 girls in South Africa, aged 16 to 17, confirmed this. Many of the girls reported that their opportunities to go out at night were restricted due to safety concerns; while kept at home for their protection, they are often participating in chat rooms with numerous people unknown to them in the physical world. The increased usage of mobile phones for going online limits the ability of parents to restrict, monitor or control how and what their children access in cyberspace.

A 2009 study in the United States determined that the pattern of mobile phone usage was highly dependent on gender. A random sample of nearly 1,000 middle-school students asked them to rate the different ways they use their cellphones. Boys scored higher than girls for playing games, sharing pictures and videos, listening to music or sending email, whereas girls scored higher for using the phone as a phone book or contact list. These findings were explained in terms of gender socialization, with boys being taught to explore and be more creative with technology and not to be afraid to take things apart, leading to more advanced cellphone use and perceptions of the phone as a ‘gadget’.

In more traditional types of mobile phone use, such as calling to talk with another person and text messaging, little difference by gender was detected; girls averaged 2 hours on the cellphone each day, and boys averaged 1.8 hours. A study in China, India, Japan, Korea and Mexico found that children who frequently communicate via mobile messaging (mobile email or short message service) consider their mobile phones to be essential; communication with friends was the primary reason for children owning a mobile phone, and text messaging was used more often than voice calls.

As of 2008, the ITU global survey found that among the 5 to 14 age group, computers were still the predominant way for children to access the Internet, with the exception of Japan. In Japan nearly 60 per cent of children access the Internet through a mobile device. It is likely that children’s use of Internet-enabled smartphones will progressively increase in most countries, depending on socio-economic conditions.

Children’s online and cyberspace activities

Social engagement online is now a fundamental part of children’s and young people’s lives. Furthermore, as the functions are beginning to merge, the boundaries between chat rooms, discussion forums, gaming, email, instant messaging and social networking sites are ceasing to have validity. Children move through these environments without constraint, and electronic service providers offer all types of
content within a single domain to capture larger shares of the market. Facebook, for example, offers one-to-one chat and online gaming; social networking sites, such as Netlog, give users the option to make their MSN Messenger ID publicly available.

Mobile phones are now used to access the Internet, text message, instant message, email, exchange images, take photos, and download music and videos – encompassing all the functions that were previously available only on a computer. Internet connectivity means that online access is no longer limited to those times when children and young people are sitting at a computer. Rather, they have the capacity to be connected when on the move, in physical contact with friends, at night in their rooms, at school and during all waking hours. This merged environment has profound implications for the nature of risk, vulnerability and potential harm.

**KEY MESSAGE**

Many activities previously undertaken via computers in fixed locations are now being done on mobile phones with Internet connectivity. When children have access to such phones, parents are less able to monitor their children’s activities, introduce filtering or blocking mechanisms or control the degree of access to the Internet.

It is difficult to obtain an accurate and comprehensive representation of activity patterns across different groups of children and in different regions. However, the ITU’s 2008 global survey identified some general patterns that indicate, for example, greater use of the Internet by children aged 5 to 14 for education and playing games than among other age groups, and heavier use for communication among youth (aged 15 to 25) and the general population.135

Children and young people are major users and creators of web content, although a significant gender gap exists, with fewer young females engaged in these activities. In the United States, a 2006 survey of 12- to 17-year-olds found that girls were more likely than boys to post photos or to write blogs and online journals, and boys were more likely to post videos.136 Across all countries in Europe, and for both girls and boys of all ages, the popular forms of Internet use are looking for information on interesting topics, browsing for fun and playing online games.137 And for many young people in the Republic of Moldova, the Russian Federation and Ukraine, communicating through email, instant messaging and voice over the Internet is a part of daily life.138

In Brazil, social networking has been found to be the favourite online activity for 80 per cent of children and adolescents, followed by instant messaging.139 And in 10 cities in India, nearly all the girls and young women responding to a survey identified school research as their primary use of the Internet, followed by entertainment.140 The pattern persists across all socio-economic categories and cities.

EU Kids Online research in 2009 found that across the 21 countries studied, boys are generally involved in a wider range of online activities and have different preferences to girls, particularly in types of downloads and gaming activities. Boys tend to go online for entertainment and are drawn to action games and sports; girls usually access adventure, party and mind-challenging games, engage in self-expression and surf the Web for educational purposes. Compared to boys, girls are more likely to use email, instant messaging and blogs; publish photos of themselves; and access a wider range of user-generated content.141

Online chat and social networking

Probably the biggest change in the way people communicate has been brought about by the emergence of social networking sites, online utilities that allow users to create profiles and form networks of friends. There are several social network sites, and their popularity varies across the world: Facebook and Twitter are popular in the United States and Europe, Orkut in Brazil and India, QQ in China, VKontakte in the Commonwealth of Independent States and the Russian Federation, and hi5 in Latin America.

The visibility of a user’s profile (basic information about the user, often including a picture) varies by site and according to her or his discretion. Sites such as Myspace allow users to choose whether they want their profile to be public or ‘friends only’. Facebook takes a different approach; by default, anyone with a Facebook account can view other people’s profiles, unless a profile owner has decided to deny permission.
Social networking sites and other online forums deconstruct traditional boundaries of privacy. They create a situation in which children engaged in ‘chat’ or ‘conversation’ in the apparently private space of their own rooms can expose themselves, wittingly or unwittingly, to an unknown worldwide audience. Warning signs that can serve to protect children in the physical world are largely absent online.

These services allow people to come together online around shared interests or causes. It can be argued that social networking sites have radically challenged our understanding of territorial networks. Traditionally, it had been estimated that in industrialized societies, the average social network comprised around 150 individuals, and that once established, it tended to change little over time.142 With social networking sites, social success and status are often defined in terms of the breadth of networks, resulting in an interest in seeing them grow.143

Furthermore, within the culture of openness promoted by social networking sites, it can be socially awkward to refuse when an offer of friendship is made; it is sometimes easier to accept, irrespective of whether that person is liked or known by the recipient of the request. Thus, one’s ‘friends’ on social networking sites may comprise people only met online and loosely connected contacts on the periphery of a person’s life as well as close longstanding friendships. While this does not mean that children cannot or do not differentiate within personal relationships, it does mean that there can sometimes be no formal distinction between online ‘friend’ relationships in terms of access to personal information, postings or types of communication.

These sites have proved to be enormously popular with young people. Since their introduction in 2003, the participation rate has grown at phenomenal speed. Facebook, launched in 2004, is one of the most popular networking sites, with 774 million users globally as of December 2011.144 Europe has the most Facebook users, with 219 million people registered;145 the top five countries are the United States (155 million users), Indonesia (40 million), India (38 million), Turkey and the United Kingdom (both 30.4 million).146 The number of Facebook users in India grew by 10 million between April and November 2011.

In the United States, 73 per cent of teenagers online in 2010 used social networking websites, up from 55 per cent in 2006.147 Also in 2010, it was estimated that 10.5 million people aged 13 to 17 were using Facebook, representing 11 per cent of the total usage.148 In India, the 13 to 17 age group represents 12 per cent of all Facebook users; the total male-to-female user ratio is 72 per cent to 28 per cent.148 In Brazil, the number of Facebook users reached 30 million by December 2011, of which 54 per cent were male and 46 per cent were female; 13 per cent were aged 13 to 17.150 In early 2011, VKontakte had more than 100 million users registered across the Russian-speaking world, though it is unclear how many are children.151

For children, and for young people in particular, the peer group is enormously important and can explain the enthusiasm and speed at which they have exploited and pushed the boundaries of virtual social networks. Children must be at least 13 to register with social networking sites such as Bebo, Facebook or Myspace, yet there has been widespread concern about enforcing this age limit – even though social networking sites have introduced safeguards to prevent young children from joining.152

A 2010 report found that 19 per cent of children in the United Kingdom aged 8 to 12 who used the Internet at home said they had a Facebook page or profile, 11 per cent said they were on Bebo, and 4 per cent on Myspace; 25 per cent of this age group had a profile on at least one of these three sites, up from 15 per cent in 2008.153 Across the European Union, 59 per cent of children aged 9–16 have a social networking profile, with the percentage increasing as they get older, from 26 per cent for age 9 to 10 to 82 per cent for age 15 to 16.154

In response to young children’s attraction to social networking, a growing number of sites are being designed specifically for them, and some are adding protection mechanisms. Habbo Hotel, for example, has 162 million registered avatars and provides automatic blocking of personal information and offensive language – along with police-vetted supervisors who are online 24 hours a day and can offer referrals to a child protection agency or specialist.155
Social networking sites are increasingly viewed by children and young people as an integral part of their social lives. They are redefining the way relationships are conducted, changing the concept of friendship, and facilitating high levels of interaction and information exchange about every aspect of daily life. Research shows that these sites provide children and young people with emotional support as well as far greater opportunities for social exchange than are available to them in traditional social forums.

In a 2006 survey in the United Kingdom, young people described the key attractions of social networking as facilitating social relationships, providing an economical (free) means of communication, access to entertainment such as humour and games, and allowing a means of expression not available offline. In addition, they said that social networking encourages creativity, enables choices and opinions to be informed by peer preferences, facilitates discussion of matters that are hard to handle face-to-face and provides a platform for self-expression with the network as the audience. The Internet has also become a vital link for lesbian, gay and transgender youth who might otherwise be isolated. However, filtering classifications are often insensitive to non-heterosexuals, creating greater restriction for such groups and increasing vulnerability in their search for social contacts and information.

**Online gaming**

Online gaming has grown enormously during recent years. Most gaming platforms, including personal computers, the latest generation of game consoles and mobile phones, offer online connectivity. Games can range from simple text-based to those incorporating complex graphics and virtual worlds populated by many players simultaneously. These are known as Massively Multiplayer Online Role Playing Games (MMORPGs). Many online games have associated Internet communities, making them a form of social activity.

The online element of gaming is still relatively new, but its popularity is increasing with Internet access and readily available broadband technology and is predicted to expand dramatically during the next few years. Research in the United Kingdom indicates that video games are among the top favourite online activities for children and young people across all age groups. Console access increases with age; among boys aged 11 to 16, some 34 per cent have online access via a games console.

Another survey suggests that 25 per cent of MMORPG players are under age 18.

**Blogging**

Blogs became popular in the years immediately following the turn of the century. Typically, they combine text, images, and links to other blogs, web pages and media related to their topics. Since 2006, blogging in the United States has dropped among teenagers and young adults significantly, while simultaneously rising among older adults. In the United States, 14 per cent of teenagers who went online in 2009 said they blog, compared to 28 per cent in 2006. Where teenagers are engaged in blogging, they do not appear to have a high level of interaction with strangers and are unlikely to be exposed to pornographic or abuse images or to be sexually solicited. There may be a greater risk, however, of online harassment among young people who use blogs because of the prevalence of peer-to-peer interaction; little data are available on such activities among young people outside the United States.

**Twitter**

Up to now there is little evidence to suggest that children and young people have embraced Twitter, a social networking and microblogging service that enables users to send and read other user messages called ‘tweets’, on a significant scale. A survey conducted in 2009 in the United States indicates that participation rates increase during the teenage years but, on average, only 8 per cent of children aged 12 to 17 were using Twitter. Older teenagers use Twitter more than younger teens: some 10 per cent of 14- to 17-year-olds compared to 5 per cent of 12- and 13-year-olds. Among high-school-aged children, girls are more likely than boys to use Twitter, at 13 per cent and 7 per cent, respectively.

Twitter’s drawback for young people appears to be that it is less secure, more public and too condensed. The public nature of Twitter may serve as a disincentive to younger users, either because they wish to hide their activities from their parents or because their parents may wish to restrict their access to strangers on the Internet. Furthermore, social networking sites already offer children the opportunities for communicating with their peers, and Twitter provides no added value. Also, teenagers largely use social networking sites for communication with friends, whereas Twitter...
is mainly used to broadcast ideas or questions and answers to the outside world, and for professional purposes and marketing – needs not felt by most teenagers.  

Chapter 4: Risk, vulnerability and harm

While there is a growing body of evidence on the nature of risk for children and young people online, it is necessary to differentiate between activities perceived as risky and the possible harm associated with those risks. A child may take or encounter risks, but not experience abuse or harm. Levels of harm are significantly lower than levels of risk. Many children, for example, may place personal information online, which many adults might characterize as risk-taking behaviour, but only a minority are likely to experience any consequential harm.

As regards the Internet there is no easy line to be drawn between activities leading to benefits and those leading to risks. It is important to recognize that there are developmental and cultural benefits for children and young people in their taking certain risks, and efforts to create risk-free environments can bring unintended negative consequences. In many industrialized countries, for example, considerable investment has been made to reduce risks in recreation and play through such things as soft surfaces, safety rails, and strengthened health and safety regulations. These measures, however, have restricted children from playing as they might wish, and an overly risk-averse culture has led to a prohibition of children climbing trees or swinging on swings without onerous risk-assessments undertaken by supervising adults.

An analogy is sometimes made with teaching children to cross the road. It is necessary both to create a safe environment with speed limits, safe crossing points and speed bumps and to educate children in the behaviours they need to adopt in order to avoid accidents. The child can then be introduced gradually to greater degrees of independence overseen by responsible adults. In the context of communication technologies, however, this analogy has significant limitations.

First, it assumes a relatively static and familiar environment in which parents can teach their children a concrete set of skills. But the Internet is not a static environment. Electronic communication and children’s usage are constantly changing – and children are active agents in that process. Adults are not always able to translate their ‘wisdom’ in understanding the nature of risks faced by children offline into successful strategies to protect them, or help them to protect themselves, in the online environment.

Second, it assumes that responsible adults understand the risks and are well equipped to educate and advise children on their nature. In fact, many adults know little about the risks associated with the Internet and the extent to which those risks lead to potential harm, especially if they themselves are not regularly online. Adults commonly lag behind children and young people in understanding the new forms and opportunities for communication and are therefore inadequately informed, not only as to what their children are doing online, but also to the risks that they might encounter.

Third, children are not merely victims, they have expertise in their own behaviours, what places them at risk, how they act to protect themselves and how they can contribute to the safety of their peers. Conversely, they can be actively engaged as perpetrators and abusers online. External protection in such forms as laws, regulations, law enforcement, filters and reporting mechanisms is still evolving and needs to be developed in partnership with children and young people in light of their own concerns and experiences in using the online environment.

Given the rapidly growing scale of usage and the centrality of online communication in children’s and young people’s lives, it is important to understand how they behave online, the types of behaviour that can place them at risk, how they perceive and understand the potential risks to which they may be exposed, if there are certain children who may be more at risk than others, and whether any conclusions can be drawn about the potential degree of any consequent harm (this last is developed further in Part Two).

Behaviour and activities carrying potential risk of harm

To date, the research available on risk-taking behaviours derives predominantly from Europe and the United States, where, overall, the degrees of risk seem positively correlated with levels of usage. In other words, the more that
children use the Internet, the more likely they are to encounter risks.

In their study of online activity in the European Union, Sonia Livingstone and Leslie Haddon of EU Kids Online have provided a useful classification of the risk and behaviours from the perspective of children, which can be summarized as:

**Content** – child as recipient of general information such as advertising or spam; violent, gruesome or hateful content; pornographic or harmful sexual content. In this context, the child has no active role in the process. Merely by being online through the computer or mobile phone, she or he receives content that has been disseminated widely and opportunistically; this content is not targeted to reach that particular child, he or she simply happens to ‘stumble across’ it.

**Contact** – child targeted as participant in one-on-one activity by another child or an adult, e.g. being bullied, harassed or stalked; tracking or harvesting personal information; unwelcome persuasion or encouragement to commit self-harm; being groomed online for sexual abuse offline or being sold online for sexual abuse both online and offline; being made the subjects of child abuse images; being abused through prostitution, using the Internet and mobile phones to contact their abusers; or being targeted to engage in cybersex.

**Conduct** – child as actor initiating abusive or risky behaviour, e.g. creating or uploading pornographic material; bullying or harassing another person; sharing personal information online; downloading sexually abusive images of children or placing images of themselves or other young people online; making ‘friends’ known only online. In this context, it is the child who is the initiator of risk-taking or abusive behaviours.169

It is necessary to distinguish between these different forms of activity. First, there are some online behaviours that involve solely the child or young person, for example, choosing to download adult pornographic images. Second, children can and do willingly share personal details and images, not only among individual friends, but also in the public domain on social networking sites. This information can trigger the attention of potential abusers.

In addition to the studies from Europe and the United States, research on young people’s usage and behaviour online has been conducted in Australia, Bahrain, Brazil, Nepal, the Philippines and South Africa. From the evidence to date, it appears that most young people who use the Internet are doing so in similar ways, particularly in respect to the role of social networking sites in their lives. The studies reveal a remarkably common pattern of social activities, perhaps indicating that factors relating to child and adolescent development are more significant than social or cultural dimensions as the driver of online communication.

There is not yet sufficient evidence, however, to provide clear indications as to whether the risks associated with these 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 social and legal protection for children and enhance potential victims’ vulnerability.170 Children in poorer countries who have access to the Internet may be particularly vulnerable to online solicitation because their economic situation may pressure them into accepting an ‘offer’ that includes payment. So far, the evidence of grooming and solicitation mainly comes from the industrialized world, but this may be an artefact of the available research and patterns of policing.

**KEY MESSAGE**

The nature and patterns of online activity seem to be broadly similar across different regions of the world. As they gain access to the electronic media, children and young people of similar ages are making use of and engaging in comparable activities. What differs is the nature of risk and harm in the context in which young people access and participate in those environments.

Furthermore, although there are some data disaggregated by age, gender and socio-economic status, there remains scarce knowledge of how children are behaving on the Internet for many groups, including children with disabilities; gay, lesbian and transgender
Child safety online

Placing information and images online

Children and young people commonly place highly personal and detailed information and images of themselves on their ‘page’ on social networking sites. What they consider acceptable to post varies among cultures.

Research in the United Kingdom discovered that children’s perceptions of what constitutes personal information may not correlate with the perceptions of adults. A 2009 study in the United Kingdom, involving 1,800 children aged 11 to 16, found that while some children would withhold telephone numbers and addresses, they would readily post pictures of themselves in their school uniforms. More than one third of young people say they have shared their age and email address with someone they only know online, and more than one in five have shared their full name, where they go to school and photos of themselves.171

Another United Kingdom survey of 695 secondary school pupils found that around a quarter of the respondents had either disclosed personal information online or had sent images to someone they met online.172 The study of 1,800 children found that girls use social networking sites and instant messaging more and are somewhat more inclined to post personal information and engage with strangers than are boys.173 In Brazil, recent evidence indicates that 46 per cent of children and adolescents consider it normal to regularly publish photos online, 30 per cent believe it is normal to publish their full family name, and 34 per cent think it is common to share private information about their daily online and offline habits.174

A study from the United States found that up to 80 per cent of children had posted their photographs online, and 93 per cent of children listed their home town.175 However, the same study revealed that only a small minority (5–11 per cent) would post more sensitive information such as their telephone number. Recent research among 2,600 young people aged 7 to 18 in Bahrain indicates that young people there commonly place personal information online and had little understanding of the concept of privacy. A significant number have their social networking site profile set to ‘public’ with no knowledge of how to set it to ‘private’. The study also found that young people aged 14 to 18 were more likely to place personal data online than those aged 11 to 13.176 Personal information can also be posted by someone else. For example, ‘tagging’ as a means of linking individuals to their digital photos, locations and events is now a widespread practice and children do not need permission from the concerned third parties (although the person who is tagged does have the option to remove the link).

Online gaming sites pose new and additional risks for children. For example, children or young people who are in contact with anyone through a social networking site profile must ‘friend’ the newcomer, and before doing so have the opportunity to scan the newcomer’s profile. They may look for personal data, photos, or the existence of common friends or networks. By contrast, when accessing or posting information on an online gaming site or a chat room, children and young people only have access to the most basic level of information or no information whatsoever about other players. In other words, on social networking sites, most young people are interacting with friends within a given network, whereas on gaming communities they are communicating with complete strangers.177

Significant numbers of young teenagers are uploading visual representations of themselves that are sexual in tone without completely understanding the perpetual nature of any image or video that is distributed online – or the ways in which these can be subsequently accessed and exploited by adult audiences for the purposes of sexual gratification. In a survey of young people in Nepal, 11 per cent claimed to have talked about sex with people they did not know, 36 per cent said they had done or said things over the Internet that they did not normally do or say, and 5 per cent admitted to exposing themselves through a webcam.178

In some places, children and young people are going beyond merely placing information and images of themselves online. In Denmark, Norway and Sweden, for instance, websites have been created that solicit male and female teenagers to film themselves and submit the images to these sites. The teens are enticed by promises of financial reward or the ‘opportunity’ to have their images judged and awarded points by the website visitors; these websites have reportedly drawn in hundreds of thousands of users in Scandinavia.179
**Online chat with ‘strangers’**

The most recent EU Kids Online survey found that a significant proportion of children and young people say they have contact with someone online who they did initially know offline, ranging from 19 per cent of respondents aged 11 to 12, to 23 per cent of those aged 13 to 14 and 33 per cent for the 15 to 16 age group. Research in Brazil indicates that 32 per cent of children and young people online have more than 30 ‘friends’ that they only know online. According to a survey of a representative sample of 8- to 19-year-olds across the United Kingdom, 27 per cent of young people have become acquainted with someone online whom they have not met before in person. This most frequently happens via social networking sites; 91 per cent of children aged 14, for example, who had met someone online said it occurred via a social networking site. The study also found that of the 27 per cent of children who had met someone online, 28 per cent went on to meet that person face-to-face. Broken down by age, 15 per cent of 8-year-olds, 15 per cent of 12-year-olds, 25 per cent of 14-year-olds and 37 per cent of 17- to 19-year-olds met an online acquaintance in person. In another study in the United Kingdom, it was reported that as many as 24 per cent of 695 students polled had met someone offline who they only knew previously from online. While the circumstances of such meetings or whether they occurred with parents’ consent are unknown, such behaviour has the potential to place children at risk of abusive behaviour. There is little reason to believe that children in the United Kingdom are unique in respect to this behaviour.

In a survey of 2,600 young people in Bahrain, 43 per cent admitted to having met with an online contact whom they had not known before in person. This research also indicated that children in public schools were more likely than those in private schools to meet people online whom they had not met offline. Specifically, girls in public schools appeared to take greater risks than their counterparts in the private education sector. The research also revealed that there is a growing pattern of young girls interacting with boys online, behaviour that is restricted in the offline environment. In this context, the risks associated with this behaviour may result from discovery by parents; in April 2010, there were seven confirmed suicides as a consequence of fear of, or actual, extreme parental reactions. The limited evidence from developing countries points to similar patterns. In Nepal, a recent survey by ECPAT International reveals that 26 per cent of girls and 73 per cent of boys admitted to giving out personal information to people online they did not know. Sixty per cent also claimed to have met virtual friends in person, of whom 15 per cent reported having had a bad experience in doing so. In Brazil, despite a majority in one survey indicating they had learned about online dangers (60 per cent), nearly half of the girls said they would meet offline with someone they had met online. In another Brazilian survey, 11 per cent claimed to have already met someone in person who they had met online, 90 per cent of them doing so alone. In the same group, 42 per cent said that they had a friend who had already met someone under those circumstances.

By contrast, research in South Africa found that girls are using chat rooms as a substitute for face-to-face interaction, which has been restricted by their parents ostensibly for their own protection from violence and risk in the their local environment. As a result, the girls are spending hours in their bedrooms in chat rooms with large networks of people, usually unknown to them in the real world. The content of the ‘chat’, however, is generally characterized by the girls as advice sharing and gossip.

Surveys conducted in 2000 and 2005 in the United States with samples of around 1,500 children aged 10 to 17 reveal some changing patterns in experiences on the Internet. The number of children using the Internet to chat, email or instant message with strangers decreased from 40 per cent to 34 per cent. Similarly, the percentage of respondents saying they had formed close friendships with people they met online declined from 16 per cent to 11 per cent. There was also a considerable decline in chat room use; from 56 per cent to 30 per cent (although this trend may reflect the fact that social networking sites are more often including a chat function).

It was also found that unwanted sexual solicitations decreased since the first survey, from 19 per cent to 13 per cent. This decrease seems partly due to young people being more cautious about interacting with strangers online, with fewer talking face-to-face to people they did not know. Regarding solicitations, 41 per cent took place when children were not alone, indicating that they are more likely to engage in risky behaviour within the apparent safety of a group of friends. Nonetheless, awareness of dangers on the Internet appears...
to have grown among young people in the United States, and that this may be behind their changed behaviour.\textsuperscript{191}

It would be helpful to have a better understanding of how such changes have come about – whether as a consequence of external messages and information provided by adults about the risks, the imposition of boundaries from parents, exposure to media coverage of high-profile cases of abuse and danger, or the internal networking and communication mechanisms among groups of young people themselves. It would also be interesting to find out whether there is an evolutionary process at work. It may be possible that the first generations of children and young people experimenting with technology and the online environment were pushing its boundaries without the benefit of experience regarding its implications. Subsequent cohorts may learn from their peers, older siblings and others about the consequences of these behaviours and begin to evolve new codes of behaviour, protective strategies and greater understanding of privacy.

\textit{Exchanging images via mobile phones}

Texting has become an increasingly common practice among teenagers during recent years. Of growing concern to many parents, teachers and professionals working with young people, at least as reflected by evidence from the United Kingdom and United States, is the extent to which more and more teenagers are using their phones as a means of sexual communication, exploration and sharing. In particular, concern has focused on ‘sexting’, the creating, sharing and forwarding of sexually suggestive nude or nearly nude images by teenagers.

A 2009 survey of 800 young people in the United States, aged 12 to 17, found that there are three main scenarios for sexting: exchange of images solely between two partners in a romantic relationship; exchanges between partners that are shared with others outside the relationship; and exchanges between people who are not yet in a relationship, but where at least one person hopes to be.\textsuperscript{192} The survey found that:

\begin{itemize}
  \item Four per cent of 12- to 17-year-olds who own mobile phones said they had sent sexually suggestive nude or nearly nude images of themselves to someone else via text messaging.
  \item Fifteen per cent of cell-owning 12- to 17-year-olds said they had received sexually suggestive nude or nearly nude images of someone they know via text messaging on their cellphone.
  \item Older teenagers were much more likely to send and receive these images.
  \item Eight per cent of 17-year-olds with cellphones had sent a sexually provocative image by text and 30 per cent had received a nude or nearly nude image on their phone. Focus group discussions suggest that sexually explicit images are being forwarded to others, for example, ex-boyfriends sharing the images with their friends, which could explain the difference between the percentages of those who send and receive these images.
  \item Teenagers who pay their own phone bills are more likely to send ‘sexts’; 17 per cent of teenagers who pay for all the costs associated with their cellphones send sexually suggestive images via text, but just 3 per cent who do not pay for or only pay for a portion of the cost of the cellphone send such images.\textsuperscript{193}
\end{itemize}

Other surveys from the United States indicate higher rates. One study from 2009 showed that one in five of 13- to 19-year-olds had sent a sexually suggestive message or nearly nude photo,\textsuperscript{194} and another that 24 per cent of 14- to 17-year-olds reported they had “been involved in some type of naked texting.”\textsuperscript{195} A 2009 Internet survey in the United Kingdom of more than 500 children aged 9 to 13 found that:

\begin{itemize}
  \item Twenty-seven per cent of children said that sexting happens regularly or all the time.
  \item Forty per cent said they had friends who took part in sexting.
  \item Fifty-six per cent were aware that images had been distributed further than the intended recipient although only 23 per cent felt that this was done to cause upset.\textsuperscript{196}
\end{itemize}

This research does not provide a breakdown of the data by sex or age, but clearly indicates that, overall, young people are well aware of the concept of sexting and a significant proportion is actively engaged in the practice.
In Latin America, there is no directly comparable available data, but the SaferNet Brasil survey indicates that 22 per cent of all participants (aged 10 to 17) said that they were ‘flirting online’ and another 12 per cent had already sent ‘sensual’ pictures of themselves either by cellphone or posted online.197

Constrcuting avatars

Another emerging Internet phenomenon is the growing number of sites where the user can construct an avatar, a self-rendered, digital representation of the user and, in many social networking sites, the fundamental avenue by which virtual identities are presented to others. Avatars provide an opportunity to present oneself in whatever guise is desired and are widely adopted in a number of online games such as World of Warcraft, the Sims and Habbo (the latter being aimed to teenagers and having more than 100 million avatars as of 2008).198

There is limited research available on the extent to which young people engage in constructing avatars or the implications when they do, although there are indications that avatar choices may affect the nature of online interaction. A survey in the United States of girls aged 14 to 17, for example, found that those who presented themselves provocatively in terms of body and clothing choices were more likely to engage in higher rates of disclosure and to have had online sexual advances. The survey results also indicated that adolescents who had experienced high levels of online sexual advances were more likely to agree to offline meetings and, in some cases, girls were aware of the potential sexual nature of the offline meeting.199

Exposure to pornography

A great deal of concern has been expressed in the media about the extent to which the Internet provides increased access to or exposure of children and young people to pornography. The growth of Internet usage has undoubtedly transformed the experience of both wanted and unwanted access. In the past, young people’s (predominantly boys) access to pornography would have been limited primarily to magazines that provide static images. The pornography to which children can be exposed online is of a fundamentally different nature to that previously generally available. Not only is it far more readily accessible, it is available on video, in more violent and extreme forms, in live time and on demand.

KEY MESSAGE

Information communication technologies have created an environment in which access to pornography has become relatively easy. Many sites display extreme forms, which are accessed, intentionally or unintentionally, by countless young people. There is, to date, limited evidence on the implications of exposure.

An almost certainly new phenomenon created by the Internet is the degree of unwanted exposure to pornography. Prior to the Internet, it was unlikely that young people would come across pornography without actively seeking it out. The evidence on exposure to both wanted and unwanted images indicates that levels of both experiences are consistently high, though patterns vary in different countries.

Although a number of studies document prevalence rates of children’s exposure to pornography, a degree of caution is necessary in interpreting the data, partly because of inconsistent definitions of pornography. If nudity in any form is viewed as pornography, for example, prevalence rates are likely to be higher than a study that defines pornographic content as a more explicit representation of sexual activity. These differing definitions may apply not only across countries, but also across communities or groups within a country. Additionally, the age of children involved in the studies is not consistent, making it impossible to draw meaningful comparisons. Finally, in societies where sexuality is openly discussed, children might be more likely to admit having viewed nudity.200

Overall, surveys seeking information on exposure to nudity or pornography might be influenced by the nature of the subject, which is generally sensitive among adults and even more so among teenagers. However, with the qualifications noted above, it is possible to gain a preliminary understanding of the levels of exposure.

In a telephone survey of a nationally representative sample of 1,500 boys and girls
aged 10 to 17 conducted in the United States, in 2005, 42 per cent of the respondents stated that they were exposed to online pornography within the past year; of those, 66 per cent encountered unwanted exposure. Teenagers in general, young people who had been harassed or sexually solicited online or bullied offline, and borderline or clinically depressed teenagers were more likely to experience unwanted exposure. Rates of wanted exposure were higher among file-sharing programme users who downloaded images and teens who talked online about sex to people they had not met offline, accessed the Internet at friends’ homes or were inclined to be rule-breakers. On the positive side, the risk of unwanted exposure to pornography was reduced by filtering and blocking software, and by attendance at an Internet safety presentation conducted by law enforcement personnel.201

A study supported by the Council of the Baltic Sea States – which drew evidence from a questionnaire responded to by 20,000 young people around 18 years old in Estonia, Lithuania, Norway, Poland, the Russian Federation and Sweden – found high levels of use of online pornography, although there were wide differences between countries and between boys and girls. Around 25.1 per cent of Norwegian boys said they accessed pornography on a weekly basis, compared with 10.4 per cent of those in Lithuania. Among girls, the levels were far lower, ranging from 0.3 per cent in Norway to 1.7 per cent in Lithuania.202 In a separate survey of more than 4,000 children aged 14 to 17 in the Russian Federation, nearly 80 per cent of the 16- to 17-year-old participants indicated that exposure to pornography was a risk for young people associated with the Internet, but it is not clear from the data whether this was a perceived risk or one they had actually experienced.203

In Brazil, the SaferNet survey revealed that 31 per cent of 10- to 17-year-olds had received sexually explicit images or films.204 A 2010 study of online behaviours of thousands of children aged 9 to 16 across Europe found that, overall, 14 per cent said they had seen sexual images online during the past 12 months; the percentages increased with age and were somewhat higher for boys than girls.205 In India, one third of 10,000 girls and young women who responded to a survey reported having received obscene calls or messages on their mobile phones. The pattern varied across cities, with nearly 75 per cent of girls from Bhubaneswar and 65 per cent from Hyderabad having received such calls. This kind of contact was cited as the primary disadvantage of using the mobile phone by two thirds of the girls.206 However, as the next section discusses, such unwanted exposure to sexually explicit messaging could be also interpreted as harassment.

In Pakistan, Internet penetration remains relatively limited but is spreading to small towns, where children can access it through Internet cafes that have individual workstations for each computer terminal, which is commonly enclosed in a wooden or cardboard cubicle to afford the web-surfer some privacy.207 A survey conducted there found that 50 per cent of boys who responded had accessed pornographic material, usually in an Internet cafe, while more than 80 per cent could name a pornographic website.208

A survey in Nepal involving 1,430 boys and girls aged 12 to 18, from both public and private schools in Bhaktapur, Kathmandu and Lalitpur Districts, also indicated high levels of exposure to pornography. Again, the majority of the young people were accessing the Internet in cybercafes. More than two thirds of respondents said that they had come across sexually explicit images or films online. Of those who had encountered pornography, about 35 per cent had done so intentionally and nearly 20 per cent reported that they viewed such materials on a regular basis. Pornographic images are downloaded onto mobile phones or pen drives and distributed among friends. Thus, younger boys who have not accessed the Internet have nonetheless viewed pornographic material on their friends’ or brothers’ ICT devices. The respondents observed that, even if they had no intention of visiting pornographic sites, they encountered pop-ups when downloading music or on other non-pornographic sites. They also received junk email with pornographic images.209

Findings of a study involving learners aged 13 to 17 in schools in Cape Town, Durban and Johannesburg revealed that 64 per cent of students reported that they had seen pornographic images on the Internet, with 70 per cent inadvertently connecting to pornographic sites, mainly through pop-ups and typing search words while surfing.210 A columnist’s study of Internet cafes in Ghana noted that they were full of 13- to 17-year-olds during school break times and after school, using their pocket money to pay for browsing the Internet where they are exposed to pornography.211
In 2005, the Republic of Korea reported growing complaints about online pornography and stated that “young Internet users are increasingly exposed to pornography, whether they wished to see it or not. The rise in the number of complaints is said to be due largely to the popularity of peer-to-peer sites, where Internet users can share personal files without having to go through an age authentication process.”

The 2008 IYAC Global Online poll found that while 10.2 per cent of respondents perceived coming across inappropriate content as a threat, 42.6 per cent said they had actually experienced it.

Many young people tended to attribute their unwanted exposures to letting their guard down, for example, explaining that the incident happened because “I spelled a word wrong,” “I guess I wasn’t being careful,” “I was not clear enough doing the search,” “I was dumb enough to click on the link” and “I didn’t read the information underneath the link.” In other words, they appear to be blaming themselves. However, some unwanted access may be a consequence of operators of pornography websites who make deliberate attempts to lure young people to them through aggressive and unethical marketing of online pornography, through pop-up and banner ads, spam, malicious software, spyware, advertising-supported software, ‘pornware’, malicious installers, hijacking and unauthorized links.

Pornography may be so pervasive that almost any kind of search might dredge it up. Technological changes may also account for the increase, including higher capacity of computers to receive, store and transmit images; the size of hard drives and the amount of memory they have available for storing data; digital subscriber lines that enable high-speed transmission over standard phone lines; and such applications as digital photography, webcams and streaming video. That said, it is important to recognize that much of the research was undertaken a number of years ago and that many of the major search engines have since become more sensitized to the problem and now include more sophisticated screening and filtering mechanisms to limit the likelihood of such unwanted access.

Bullying and harassment

Bullying has traditionally been defined as a child being the target of behaviour that is harmful or intended to harm, occurs repeatedly and involves an imbalance of power that prevents the victim from challenging or ending the behaviour. Typically, it might take place face-to-face on route to or at school. However, ICTs now provide new ‘opportunities’ for children and young people to bully others. In survey after survey, children identify this as a serious issue, even if, in Europe at least, more bullying still takes place offline than online.

Based on research with children, bullying online – cyberbullying or online harassment – is an important issue for them. Bullying online or ‘cyberbullying’ can take different forms, including threats and intimidation; harassment or ‘cyberstalking’, such as repeatedly sending unwanted texts or instant messages; vilification and defamation; exclusion or peer rejection; impersonation; unauthorized publication of private information or images; and manipulation. Bullies can also engage in taking what are sometimes referred to in the UK as ‘happy slapping’ images, acts of physical or sexual violence filmed and then uploaded and disseminated.

**KEY MESSAGE**

Cyberbullying is a major concern for many children and young people.

From the perspective of the bully, it is relatively risk free because it can be done anonymously and at a distance, and lacks sanction or supervision. Cyberbullying can also involve a lack of real awareness of the severity of its impact.

A number of characteristics of online technologies facilitate abusive or harmful activities. Unlike in the physical world, electronic bullies are able to remain virtually anonymous, using temporary email accounts, pseudonyms in chat rooms, instant messaging programmes, cellphone text messaging and other Internet venues to mask their identity. This anonymity appears to lead to fewer constraints and inhibitions, and thwart supervision over bullying behaviour. It may also take less effort to act hurtfully in cyberspace than when face to face with a potential victim.
While some cyberbullying is clearly deliberate and aggressive, sometimes it is unintentional and the result of simply not thinking about the consequences. Behaviours experienced as bullying by the victim are often not recognized as such by the perpetrator; the online environment sometimes serves to desensitize young people to the consequences of their behaviours. What may be sent as a joke may not be received as one, and the distance technology allows in communication means the sender may not see the impact of the message on the receiver. There is also less opportunity for either party to resolve any misunderstanding or to feel empathy.

Cyberbullying allows bystanders to become perpetrators by passing on or showing others images designed to humiliate, or by taking part in online “polls” or discussion groups with similar intent. They may not recognize this behaviour as bullying, but it may nevertheless cause harm to the recipient. There is conflicting evidence from different parts of the world of the levels of bullying and harassment of children taking place online, but research repeatedly indicates that it is an important issue for significant numbers of children. A 2008 study undertaken in the United States analysed the responses of 1,378 adolescents under age 18 about cyberbullying victimization and offending and found that:

- Almost 33 per cent of the boys and more than 36 per cent of the girls reported that they had been a victim of cyberbullying, predominantly through chat rooms.
- Some 18 per cent of the boys and almost 16 per cent of the girls admitted to taking part in cyberbullying, again primarily through chat rooms.
- No statistically significant differences appeared among perpetrators or victims in terms of race or gender. Boys and girls as well as white and non-white children were equally likely to engage in or suffer from cyberbullying.

According to a 2005 United Kingdom survey of 770 youths aged 11 to 19, 20 per cent of respondents revealed that they had been bullied via electronic means. Almost three quarters stated that they knew the bully, while 26 per cent stated that the offender was a stranger. Additionally, 10 per cent of respondents indicated that another person had taken a picture or video of them via a mobile phone, which made them uncomfortable, embarrassed or threatened. Of the total respondents, 41 per cent told a friend about experiencing abuse, 28 per cent did not tell anyone, 24 per cent told a parent, and 14 per cent told a teacher. The survey suggests that some young people may be reluctant to report such abuse because they fear that their parents will take the phone away. These findings were similar to those of an ECPAT International report in 2005, which pointed out that children were concerned that disclosing bullying might result in losing access to their phones or computers.

However, although cyberbullying is highlighted as an issue of considerable concern to children and young people, some larger more recent studies suggest that actual prevalence rates are lower than those reported in earlier surveys. The nationwide Australian Covert Bullying Prevalence Survey in 2009, for example, found that rates ranged from 4.9 per cent of students in Year Four (aged 8 to 9) and 7.8 per cent in Year Nine (aged 13 to 14) reporting cyberbullying. A meta-analysis from European Union countries in 2011 found that 6 per cent of 9- to 16-year-olds reported experiencing cyberbullying, with a nearly equal representation of boys and girls.

In Brazil, a 2009 online survey with a nationally representative participation of 2,525 boys and girls aged 10 to 17 indicated that more than 48 per cent had a friend who was victim of cyberbullying, 30 per cent expressed a fear of being cyberbullied, and 7 per cent had themselves been a victim at some time. Recent research in Bahrain found that children aged 7 to 18 reported that cyberbullying was a major problem, particularly in private as opposed to public schools, and this concern was reaffirmed as a serious issue by teachers. The ‘Digital Manifesto’ published by the United Kingdom-based Children’s Charities’ Coalition on Internet Safety underscores the fact that of the recognized risks to children on the Internet, “the most prevalent form of problematic behaviour online that children and young people have to face is bullying.”

Evidence on the behaviours of girls and boys is inconsistent. Some studies have found that girls are more likely to bully, others have found the opposite. A United Kingdom 2008 survey of 2,094 secondary school pupils on behalf of Beatbullying found that there was an equal division between boys and girls, but that they tended to adopt different ways of bullying. This survey also revealed that a significant number of children had both bullied and been bullied online and that cyberbullying
incorporated considerable social interaction not intended to be or not interpreted as acts of bullying by young people. In other words, much behaviour reflects a lack of awareness about the nature of bullying and a lack of understanding as regards its consequences.

The same survey indicated that in relationship to persistent cyberbullying, the risk was more prevalent among certain traditionally ‘vulnerable’ groups of children. Minority ethnic groups were found to be more vulnerable than white British. Nearly one quarter of young people (24 per cent) from ethnic groups, including Roma, Traveller of Irish Heritage, European and East European, were persistently cyberbullied compared to 11 per cent of those in the ‘white British’ category. Young people who described themselves as ‘mixed’ (19 per cent) or ‘Chinese’ (15 per cent) were also more likely to be persistently cyberbullied. The majority (62 per cent) of those children who were being persistently cyberbullied said they experienced it as an extension of offline bullying. These findings lend weight to the ‘migration theory’ according to which bullying tends to originate in traditional settings and then follow the victim online.230

The relationship between bullying and being bullied is complex. A 2008 study in the United States found that respondents who had already experienced offline bullying or problems at school were more likely to experience cyberbullying, both as a perpetrator and a victim. Equally, those respondents who bullied others or were bullied offline during the past six months were 2.5 times more likely either to cyberbully or be cyberbullied.231

Evidence from the United States also confirms high risks among already vulnerable groups and suggests that high levels of cyberbullying are experienced by lesbian, gay, bisexual and transgender young people. STOPtechNObullying.org, for example, cites department of health statistics that 54 per cent of young people in these groups have been subjected to such abuse. Furthermore, there appears to be a sense of helplessness among the victims: 49 per cent said that their parents would not believe the abuse happened, 55 per cent thought that their parents were unable to do anything about it, and 25 per cent felt that they had to deal with cyberbullying alone.232

Although the data reveal varying and sometimes contradictory results – and there are currently significant gaps in research, for example, on the prevalence of cyberbullying in developing countries – common themes can be extracted from the data available to date:

- Cyberbullying is a significant concern for children and young people.
- Unlike traditional bullying, cyberbullying is not limited by time or space and can be anonymous.
- Many children do not consider such behaviour as saying hurtful things or sharing humiliating images to constitute bullying because it took place online rather than face-to-face.
- Cyberbullying can rapidly draw in a larger audience than is ever possible with offline bullying.
- Cyberspace is a domain that offers both public interaction and perceived anonymity. This creates greater opportunity for young people to engage with their peers, often doing things they would not do in person and attempting to do so under the cover of a username (the ‘public’ name used to identify each person online, and required for access to networks and services, but not necessarily related to the individual’s given name).
- Cyberspace widens the opportunity for a greater range and intensity of bullying and can create an environment in which victims of child-on-child violence may also be harder to reach.

**Perceptions of risk, vulnerability and harm**

**How children and young people define risk**

Adolescence is a period in life when risk-taking behaviour tends to be more common. The extent to which this takes place, however, varies across cultures. In many industrialized countries, in particular, adolescents may engage in socially disapproved behaviours that entail risks to their long-term well-being.233 The online medium provides different opportunities, and consequences, for such risk-taking behaviour. Information and communication technology creates far wider access to information, exchange and social contact. It also affords the capacity for self-producing erotic material, such as images and video, participating in sexually
themed chat and engaging in sex acts while using webcams. These behaviours may not be perceived as risky by young people themselves, although parents and other adults in their lives may very well see them as perilous.

It is also important to recognize that when it comes to being online young people are likely to have a different definition of a ‘stranger’ than their parents. Young people do not consider those they have communicated with online over time as strangers; instead they view them as their online or virtual friends. Hence, young people are often willing to share information or talk to people who are only known online. Educational messages that warn children about the risks associated with meeting strangers may therefore be skewed.

In the physical world, a range of barriers – geographical constraints, parental supervision, law enforcement, the physical persona or cues of a potential ‘friend’ – serve to protect children from abuse or provide warning triggers. In the virtual world, these barriers are absent. The many mechanisms that have been developed to safeguard children in the offline environment are absent or not fully implemented in the online world.

Children’s overall level of perceived vulnerability online

Children and young people’s perception of their vulnerability to harm is related to the context in which they experience the online environment. A survey on online safety and security undertaken by the IYAC found that nearly 52 per cent of respondents reported that they felt safe online and able to cope with threats or nuisances. Computer viruses and spyware (software that allows users to retrieve information covertly from another person’s hard drive) were perceived to be the biggest threat online, selected by nearly 38 per cent of respondents. In much of the lower income world, however, cybercafes are the primary route through which many children and young people access the Internet. These environments pose additional forms of risk and potential harm. Children who rely on Internet cafes are likely to identify it as an environment where they are exposed to unregulated pornography, a lack of any filters or blocking mechanisms and where, in some cases, cafe owners provide private rooms for customers to engage in sexual activity.

A study in the Philippines found that some Internet cafes were venues where children and adults were engaging in sexually explicit conduct with their ‘chat-mates’ and were used as a forum for widespread consumption, voluntarily or involuntarily, of pornographic materials by children and young people. In Brazil, many adolescent girls said that there were no risks in accessing the Web at home or in a cybercafe, but others perceived a wide range of dangers, including cellphone theft, passwords or online profiles being copied, illegal drugs, rape, kidnappings and shootings. Both studies, however, pointed to the fact that young people feel safer in public places when they are with people they can trust and who can protect them.

In a survey undertaken by SaferNet Brasil, with 1,502 students aged 10 to 17 participating, the top two major risks of being online were perceived as data or identity theft (65 per cent) and encountering violent/adult content (56 per cent). In a study in India with 10,000 girls and young women aged 14 to 21, nearly two thirds reported fraudulent use of personal information as a potential consequence of online use, while others named access to pornographic sites, harassment and misuse of webcams in cybercafes. They also reported pop-up sites as being potentially harmful and identified webcams at cybercafes as dangerous, with the possibility of their photograph being taken during a webcam chat session and later passed around; only a very small percentage, however, had personal knowledge of actual instances of such harm.

In South Africa, in a survey of more than 900 teenagers, 73 per cent stated that they recognized that exposure to pornography can be harmful, with 13- and 14-year-olds more concerned about negative effects than those aged 15 to 17.

Internet use can give the appearance that the person online is safe and in control. But some young survivors of Internet-related abuse have likened the experience to a staircase where each step leads to new dangers – and the normal warning signs to alert the young person to the increasing risk, such as the age of a ‘friend’, are absent. Based on work with children in Sweden who have experienced Internet-related abuse, Anders Nyman has identified the following steps to potential harm:

- Revealing personal data, such as name, passwords, phone number, address or special secrets;
- Chatting about sexual matters with an unknown person;
● Uploading or sharing sexually suggestive or explicit pictures of oneself or one’s friends;

● Becoming involved in live webcam sex with an unknown person;

● Dating someone offline who was met online;

● Knowingly dating adults offline who were met online;

● Sending pictures for payment;

● Posing live on the webcam or having webcam sex for payment;

● Dating offline someone met online and having sex for payment;

● Offering sex offline and online for payment.242

In a 2006 consultation with boys and girls aged 10 to 15 undertaken by CEOP, the general perception was largely that ‘other’ groups of young people were at risk but not themselves. In particular, the respondents felt that ‘weak’ or ‘vulnerable’ children – particularly young, inexperienced users and girls – were most at risk of victimization.243 Girls aged 10 to 14 in the Brazil survey pointed to a broad range of potential online dangers, including child abuse, harassment, deception, threats, violence, paedophiles, videos and blackmail. But they had a much more limited view of the risks they themselves faced, identifying only people not being who they say they were, photos being spread around and false social networking site pages.244

In a survey by CEOP on risk-taking, young people in the United Kingdom did identify downsides associated with social networking sites, which most of them had risk but not themselves. They had a reasonably high level of awareness of potential risks associated with information sharing. As reported by the survey, their concerns included:

● Insecurity of information – younger users felt that information they posted on sites, particularly ‘private’ images and personal information, was not secure, confidential and ‘gets put on the Web’.

● Pressure to share information – many said they often felt compelled by other group members to hand out personal information, especially email addresses, when they did not feel comfortable in doing so.

● Exposure to an unwanted audience – young people felt visible to a large audience that was unknown to them.

● Unfamiliarity with people they are connecting with – some young people found it difficult to foster trusting relationships online with people they did not know offline and were concerned because they could not authenticate the identity of those they were communicating with.

● Exposure to unwanted information such as pop-ups and banners.245

It is not clear, however, how far these concerns actually influenced their behaviour. Most users stated that they would continue to use social networking sites regardless of whether the sites dealt with reported abuses unless they directly experienced a serious problem. They further stated that they were willing to overlook potential risks because of the numerous benefits of social networking sites, their dependency on interacting through these sites and the inconvenience of creating new profiles. The majority felt that they could adequately protect themselves online.246

Overall, there are widely differing perceptions among children and young people about the dangers associated with the Internet. Although the dearth of comparative research makes it difficult to ascertain how these differences arise, they seem to relate to the availability of information, awareness of safe-reporting mechanisms and location of use. Internet cafes, for example, are likely to present greater risks along with the likelihood that, in the countries where children are reliant on Internet access through cybercafes, there is less regulation, opportunity for reporting problems, parental awareness and, in many cases, overall investment in building a protective environment.

Parents’ perceptions of risk and vulnerability

In many industrialized countries, there is a high level of anxiety about children’s Internet activity among parents, and the perceived level of risk appears to be increasing. In a 2006 Eurobarometer public opinion survey across the European Union, 18 per cent of parents said that their child had encountered illegal or harmful material online, but 66 per cent felt that their children would know what to do if faced with a situation that made them feel uncomfortable.247
The 2009 Eurobarometer survey found that well over half of parents who had a child aged 6 to 17 were worried about their child seeing explicitly sexual or violent images online, being groomed or being bullied. Parents were worried more about girls and younger children, despite the fact that boys and older children take greater risks in online conduct, largely through seeking out pornographic content, giving out personal information or meeting someone offline that they have met online.\(^{248}\)

Research in the United Kingdom, published in December 2009, found that parents were consistently more anxious than their children about the degree of risk. For example, 47 per cent of parents with a child aged 12 to 17 were worried about their child being exposed to inappropriate contact on the Internet, and 42 per cent worried about inappropriate or harmful content. For children in this age group, the figures were 30 per cent and 9 per cent, respectively.\(^{249}\)

The EU Kids Online research, however, paints an even more nuanced picture, with perceptions of risks that children may encounter on the Internet being similar between children and their parents. This level of agreement, however, appears to apply only where children have not actually encountered such risks: 40 per cent of parents whose child had seen sexual images online said that he or she had not seen such images, and 56 per cent of parents whose child had received nasty or hurtful messages stated that their child had not received these types of messages.\(^{250}\)

Parental approaches to mediating children’s activity online vary significantly across cultures. Parents throughout Europe, for example, adopt a range of strategies to protect their children, including:

- Imposing rules and restrictions on access, such as limiting the hours of usage or moving computers used by children out of their bedrooms and into communal areas in the home, where parents and other family members can observe their online behaviour;

- Engaging with their children by sharing online experiences, talking and watching together;

- Introducing barrier technology such as filters and monitoring that create boundaries on the sites that children can access.\(^{251}\)

The extent to which these strategies are applied may generally be culturally determined. Nordic parents, for instance, tend not to fret about their children’s online behaviour, possibly because they have a less hands-on approach to monitoring the Internet or greater confidence in their children. Danish and Swedish parents are less likely to keep track of their children’s Internet use than parents in Germany, Greece, Ireland, Italy, Portugal, Spain and the United Kingdom.\(^{252}\) In Southern Europe, parents tend to adopt more restrictive approaches, and in parts of the Middle East the conventional view is that parents should be very controlling. In Yemen, for example, education specialists maintain that parents should ensure that their children use scientific and educational websites only and that parents should keep constant vigilance over their children’s Internet use, beginning from an early age, as they believe that children cannot distinguish between right and wrong and may be unduly influenced.\(^{253}\)

There is considerable variance between those parenting models that place more reliance on children’s own resilience and competence to act safely and protect themselves and those that see the necessity for protection exclusively provided by adults. The challenge for those who place the emphasis on protection by adults is whether in reality such a model can be effective in the context of the fast-changing online environment, especially where parents lack understanding of the Internet and the role it plays in their children’s lives. Conversely, the challenge for those who place trust in their children is ensuring that this trust is well placed and that children are socially and technically empowered and supported to be able to look after themselves and others.

A significant disparity exists between children’s and parents’ reporting of the extent of parental mediation, with children consistently reporting that it is lower than claimed by parents. The ITU, for example, reported in 2009 that 92 per cent of parents state they have established rules for their children’s online activity, yet 34 per cent of children say their parents have not.\(^{254}\) Of the respondents to the IYAC global online poll, 74.4 per cent said they had no parental restrictions regarding forbidden sites or time spent on the Internet. Additionally, 40.5 per cent stated that what they did online was rarely discussed and of little interest to their parents, but 30.5 per cent said they were open about the sites they frequented and regularly discussed their concerns with their parents or guardians.\(^{255}\)
Where parents monitored online behaviour, nearly 39 per cent of children claimed to favour their parents’ intervention and understood their motivation, whereas 28 per cent saw such parental controls as a lack of trust. In the 2010 Voices of Youth survey, 68 per cent of respondents said that their parents did not restrict their Internet usage. Of the 32 per cent who had some restrictions, most accepted their legitimacy. More recently, the EU Kids Online survey found a growing number of children who talk with their parents when upset by something that has happened online, although there is a significant difference in what they are willing to discuss: 25 per cent of children who were bothered by seeing sexual images online discussed the experience with parents, but 42 per cent of those affected by online bullying discussed it with their father or mother.

**Vulnerability to sexual solicitation**

Children and adolescents are not simply the targets of adult Internet creations; they are active participants in creating their own cybercultures. The Internet is a useful tool for children and young people who are developing their sense of identity, including testing out their sexuality. They are able to search out relevant sources of information and to discuss their emerging sexuality anonymously.

Although sharing information online, including sexualized material, has become commonplace behaviour for young people, and the risks of having potentially dangerous contacts offline are perceived by many children as real, they seem to be able to deal with these risks and avoid being harmed. But it is certainly possible that many children and young people are operating on the Internet with concepts of boundary and privacy derived from the physical world, which cannot and do not apply in the online environment. Behaviours that would not expose them to risk in the physical world can take on different implications when shared online. For example, sharing your name, address, telephone number and photo with a group of friends at school is very different from posting that information on the Internet where potentially it can be accessed by a wide audience of unknown people.

**KEY MESSAGE**

Placing personal information online is becoming normal behaviour among young people. The research evidence, however, is that it is willingness to communicate with unknown individuals rather than the placing of information per se that leads to harm.

As described above, the placement of personal material on social networking sites is commonly identified as risk-taking behaviour. 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. Basically, if a young person is not posting personal information, peers are not going to regard an SNS page as lively or interesting. They may even regard the child as being a little odd or stand-offish. Putting information online is part of the cultural mix and therefore commonplace and the majority of young people do not appear to be harmed by it. Research from the United States, for example, has found that there is little evidence that the placement of information or images online itself leads to harm; this research suggests that harm occurs only in the context of other forms of online risk-taking behaviour.

In other words, it is not the placement of material but the willingness to communicate with unknown individuals responding to that information that has the potential to place a child at risk.

Other evidence from the United States suggests that most teenagers there have a fairly clear understanding of the potential dangers online. The risks they take appear not to be a consequence of innocence, but rather that as they get older they become more sexually curious and experimental. Whereas in the past, the expression of this behaviour would take place in the physical world, the Internet now offers new and exciting opportunities to explore online. It is the isolation and secrecy of these contacts, without oversight by peers or family that can lead to relationships quickly intensifying and transferring to face-to-face contact. The challenge in many of these relationships is neither innocence about sex nor that they involve violence or force. But rather, they draw young people into premature sexual engagement with persons,
including sexual abusers, with whom they want a romantic relationship – without having the maturity to understand or handle such relationships safely.264

Few studies have been carried out regarding the number of children who are abused through grooming online. One Swedish study examined the number of 15-year-olds across the country who had received requests for sexual online meetings and offline encounters. Of the 7,500 respondents,265 48 per cent of the girls and 18 per cent of the boys claimed that they had received such a request from an adult, including requests to strip or to watch an adult masturbating in front of a webcam. These incidents were reported as common, that they happened constantly when using chat sites, and that the adult would make requests for such activities at the onset of the conversation.266

In the same study, police reports of crimes against children committed via new technologies were examined. Fifty per cent of the reported crimes only occurred online, mostly involving requests for images or for webcam contacts; the other reported crimes were committed offline, but contact was established on the Internet. In half of the offline crimes, the victim met with the perpetrator knowing that the meeting would lead to sex; the remainder were crimes where the victim thought that the meeting would be of a completely different character.267

In another study about online grooming in Sweden, involving more than 100 girls who had gone on to meet men offline, all knew they were meeting the man in order to have sex, although none of the girls would admit to being fully aware of what this would imply. It appears that something in the chat conversations with the girls made the perpetrator aware that they had vulnerabilities, ranging from loneliness to suicidal thoughts.268

Examinations of computers and mobile phones that belonged to offenders in the United Kingdom have identified changes in the manner in which some victims engage with their abusers. Young people have sometimes required the minimum of grooming and have themselves been sexually ‘upfront’ with their contact, holding conversations in which they are quite explicit regarding sexual matters.269 In other cases, there appears to be little evidence of sexual inhibitions on the part of the young person. Victims often report that they found their online ‘friends’ to be normal and felt that they knew them. These emerging phenomena have led to new terms in the literature surrounding violence against children in cyberspace, such as compliant victimization and self-sexual exploitation.270

The degree of risk for potential abuse can be compounded by the fact that abusers who use new technologies are resorting to different strategies to silence or co-opt children. The abuser may show them images of other children being abused in order to normalize the activity, show them the children’s own images, and encourage them to place images of themselves online, or encourage them to introduce their friends or be proactive in abusing other children. These strategies serve to make victims feel responsible for their own abuse and less likely to seek help because they fear they will be seen as complicit and positively engaged in the abuse activities.271

Overall, the publicity about online ‘predators’ luring innocent children through lies about age or gender misrepresents the overall picture of online predatory behaviour. Rather, the evidence indicates that Internet sex crimes involving adults and children are more likely to fit a model of statutory rape – involving adult offenders who meet, develop relationships with and openly seduce underage teenagers, rather than a process of forced sexual assault, age deception or paedophilic child abuse. This is a serious issue and one that requires different approaches from current prevention messages, which emphasize parental control and the dangers of divulging personal information.272

Thus far, the research findings as to which children are particularly vulnerable to online grooming or solicitation provide mixed messages. Some evidence points to particular groups of children being vulnerable as a consequence of difficult socio-economic circumstances or because they have already experienced sexual abuse or exploitation. Other contributory factors include alienation from parents, low self-esteem and lack of confidence. Gender is also relevant, with more girls than boys appearing to be harmed through online communication, although boys are beginning to feature more often in child abuse images online.273

Extreme poverty is likely to be a factor encouraging children to respond to sexual solicitation, particularly when combined with the likelihood of parents’ lacking the information and understanding of the online environment necessary to offer effective guidance, support or protection. In South Africa, for example, it
was found that there was some indication that children without adult supervision, like those living and working on the street, are particularly vulnerable to online sexual exploitation. As has already been described, children using Internet cafes – which are an important access point for poorer children – can be exposed both to a more sexually explicit, unregulated environment and to direct approaches by men using pornographic sites in the cafes.

Vulnerability cannot be reduced to economics alone, and research in Brazil points to the importance of considering social factors as well. Girls from favelas (low income neighbourhoods) – who appear to become more sexualized at a younger age than their peers in private school – were more likely to socialize with older age groups, whom they perceived as raising their social status, and to engage in risky behaviour with little regard for immediate consequences. Whereas the middle-class girls attending private school tended to have computers and cellphones at home and lived in an environment where they described their activities online as being focused to some extent on education, the girls in the favelas cited using the Internet to visit sexually oriented sites and to meet boys.

A 2007 study in South Africa found that exposure to online contact with predators was more likely to occur when children’s self-esteem is low and they are in need of comfort. Abusers detected these signs and manipulated the child as part of the grooming process. It also found that the children most likely to be involved as subjects in the production of child abuse images were those who had formed an established relationship with an abuser as well as those who lacked supervision. A 2004 survey conducted by UK Children Go Online found that children and teenagers who had online skills but were less satisfied with their lives than other young people, felt more confident online than offline and were more likely to give out personal information, seek personal advice, make friends online and go to offline meetings with these new friends.

Research from the United Kingdom and other industrialized counties points to a complex pattern in which individual vulnerability is not neatly associated with measures of deprivation. A CEOP analysis of children who had been victimized online found that some children had already been sexually abused offline (lending credence to the ‘migration’ theory discussed previously), while others shared no apparent negative prior life circumstances and appeared to have been randomly targeted by offenders through a range of social networking sites, chat rooms and online gaming.

There is increasing evidence from criminal investigators and those assisting children who have been abused online with their recovery that there is no typical victim and that the most striking thing about children abused online is their heterogeneity. This finding aligns with what is known about the perpetrators and victims of sexual abuse offline: perpetrators come from all walks of life, and their victims are a similarly heterogeneous group, often related or well known to their abuser.

Research by Tink Palmer in the United Kingdom appears to confirm these findings. In her study of young women aged 14 to 15 years who had been victims of grooming, none could be perceived as vulnerable in their offline world. They came from stable families reflecting a wide range of socio-economic circumstances, were of average or above intellectual ability, had no physical or mental disabilities or history of mental disturbance, enjoyed the company of their peers and were seen as capable students within their school settings. Despite the lack of offline vulnerability indicators, they became online prey to males and took risks that led to all of them being abused online, and in the case of half the sample, offline as well.

There is also increasing evidence that risky behaviours online tend to commence with the onset of puberty. All of the girls in Palmer’s study, for example, began their online relationships with predatory men when they were 12 to 14 years old. This would imply that some children may be more vulnerable to online risks during particular stages of their development.

**KEY MESSAGE**

The risks associated with the online environment are different based on the socio-economic status of children and their families. Poverty can serve as a driver to respond to approaches from predatory sexual abusers for financial gain, but middle-class children from well-off backgrounds can also be vulnerable.
Potential impact

There is only limited evidence to date regarding the impact of online behaviours. Our understanding of the damage of sexual abuse on children’s emotional and psychological well-being, for example, has grown rapidly during the past 20 years; yet corresponding knowledge on how children are affected by online sexual abuse remains sparse.282 A consideration is whether the effects are different for children when they are victims of sexual abuse in which the new technologies are the conduit. From our current knowledge, the traumatic nature of sexual abuse per se does not change if a child has been sexually abused online. Instead, it takes on a new dimension, partly because of the very nature of the Internet – for example, the fact that images may remain online for perpetuity – and partly because children become far less inhibited in what they say and do online than they tend to be offline and may therefore feel that they are responsible for placing themselves in harm’s way (this topic is considered more fully in Part Two).

Impact of exposure to pornography

The impact of exposure to Internet pornography is not clear from the evidence available to date, but some researchers have expressed concern that exposure to online pornography during adolescence, given that it is both quantitatively and qualitatively different from most other sources of access available to teenagers, may lead to a variety of negative consequences. These may include undermining accepted social values and attitudes about sexual behaviour, earlier and promiscuous sexual activity, sexual deviancy, sexual offending and sexually compulsive behaviour.

Several factors will influence how pornography affects children and young people. Individual characteristics such as age, gender, levels of parental involvement and the emotional state of the viewer at the time of watching are all relevant. In addition, the character and circumstances of exposure will have influencing effects. Thus, the amount of time spent viewing, whether the young person is alone or with others and the cultural environment in which she or he lives are all likely to determine the use, impact and meaning of pornography.283

High levels of usage of pornography by children and young people have been shown to desensitize them to violence and sexually aggressive acts, to diminish their sympathy for rape victims and to ingrain gender stereotypes.284 There appears to be consistent evidence that exposure to or consumption of pornography, particularly violent pornography, is linked with male aggression towards women.285

Questions have been raised as to whether Internet pornography influences how boys view girls, and their expectations or assumptions about girls’ bodies and how girls should behave sexually. A growing demand among young women for vaginal surgery, for example, has been linked to their boyfriends’ expectations of ‘normality’ as defined through their online experience of pornography.286 There is anecdotal evidence of abusive behaviours associated with Internet exposure to pornography among children. In Cambodia, for example, two boys in their early teens were reported to have raped a 7-year-old girl in 2003 after seeing a pornographic video.287 A study of young people aged 14 to 19, conducted in Italy, found an association between using pornography, sexually harassing a peer or forcing someone into having sex.288 Other studies show that some users and traders of child abuse images are under age 18 or in their early adulthood.289

Examples exist of children creating pornographic images of themselves and disseminating them in cyberspace.290 In 2003, in Australia, 90 per cent of 101 children under age 10 and attending a hospital child-at-risk assessment unit for sexually abusive behaviour were reported to have had regularly seen sexually explicit images online.291 In New Zealand two studies of adolescent boys referred for treatment following their arrest for possession and distribution of child abuse images reported that half the sample said they first used the Internet to view adult pornography.292

Recent developments in understanding trauma and other stimuli on the brain development of children and young people have some relevance to the debates on children’s exposure to pornography. Work undertaken by Norman Doidge states that the brain is not ‘hardwired’ but can change its own structure and function through thought and activity. He suggests that the neuroplasticity of the brain leads to brief windows of time, including puberty, when new brain systems and maps develop with the help of stimulation from the people in one’s environment and that this needs consideration when measuring the impact of pornography on adolescents.293 Clinicians appear to be
dealing with growing numbers of cases of young adults concerned about their viewing of pornography. In recent years, cases of young men (aged around 20 to 22) have arisen that require assistance due to inappropriate sexual expectations regarding their partners or inappropriate behaviours relating to pornography viewing within the family home.294

There is little adequate research on children or adults regarding the effects of unwanted or unexpected exposure. What research has been done relates largely to voluntary and anticipated exposure. The nature of the potential risk with inadvertent exposure is that the material received may be inappropriate, distressing and disturbing for the child. The degree of harm will depend on how frequently they are exposed to such images; whether they receive them when alone or with groups of friends; the environment in which the child receives such images, for example, whether at home or in an Internet cafe; and how extreme or unpleasant the content is to the child. It will also depend on the extent to which the child feels able to control the online environment to limit their exposure to such images.

Exposure to unwanted pornography appears to have varying effects in different cultural environments, with children in more socially conservative cultures being more negatively affected. Studies in the United Kingdom and the United States, for example, found that the majority of young people do not appear to be particularly upset by exposure to unwanted sexual images, possibly because many are inured by high-level exposure to related images in other contexts such as magazines, films and television.

Ven-hwei Lo and Ran Wei, in their 2005 study of Taiwanese adolescents, found that 38 per cent had some exposure to pornography online and that this was associated with greater likelihood of sexually permissive behaviours and acceptance of such behaviours.295 In the EU Kids Online survey of 9- to 16-year-olds in 25 countries, 32 per cent of those who had encountered unwanted sexual images online reported being upset by the experience. There was some variation across countries, however, with the percentage of children who said they were disturbed by these images ranging from 15 per cent in Greece and Slovenia to 49 per cent in Estonia and Turkey.296

In developing countries, where children and young people may have less exposure to pornography in the physical world, the impact may be greater. In Nepal, for example, 39 per cent of surveyed 12- to 18-year-olds reported being shocked when they first encountered sexually explicit materials.297 In addition, many are using Internet cafes, where they are exposed to other users viewing pornography, which can cause them extreme distress. The lack of filtering and blocking mechanisms in many cybercafes increases the risk of unwanted exposure. Other research in Nepal found that 92 per cent of cybercafes allowed visitors to browse any website they wished, even though 39 per cent of users are under age 19.298 However, 67 per cent of cybercafes in Nepal did block adware and pop-ups. Among 13- to 17-year-olds who responded to a questionnaire in South Africa, 52 per cent reported that, when coming across pornography online, they looked at the images before exiting the site, and 38 per cent reported that they were ‘not bothered’ by the pornographic images they came across.299 However, 73 per cent agreed that watching pornography has harmful effects on people, arguing that it exposes children to something they are not emotionally ready for and indirectly encourages them to become sexually active at a young age. Younger children (aged 13 to 14) felt more strongly about the possible harmful effects.300

Overall, young people report comparatively low levels of concern when faced with unwanted pornography, but it is possible that it has a greater impact on some young people than voluntary exposure. Some may be psychologically and developmentally unprepared for unwanted exposure, and online images may be more graphic and extreme than pornography available from other sources.

Exposure to adult pornography can form part of an abuser’s repertoire of tactics for grooming children online. By introducing the child to adult pornography, the abuser seeks to lower the child’s inhibitions about sex, including inhibitions the child might have about being used to make pornography. There is often a progression from ‘mainstream’ adult pornography to hard-core pornography and on to encouraging the child to view abusive images of children. Grooming in these circumstances has two aims: to desensitize the young person to sexual activities that may become increasingly abusive; and to feed the groomer’s fantasies of introducing a child to this material, while encouraging the child to develop masturbatory fantasies fuelled by the images. Adult pornography is also used by the abuser as a way of demonstrating ‘preferred’ or
fantasized sexual activity to the child and as a demonstration of the activity the child is being groomed to perform.

**Impact of cyberbullying**

An abundance of research has been undertaken regarding the harmful effects of bullying on children. Targets of bullying will commonly experience distress, anxiety, confusion, anger, insecurity and lowered self-esteem. In addition, they may have somatic symptoms as well as physical injuries. Children may suffer academically, possibly as a consequence of poor attendance at school or because their psychological reactions prevent them from learning or concentrating at school.

Cyberbullying has the potential to harm in profound ways. Physical bullying usually takes place when the child is in a public space and exposed to other children. The existence of cyberspace and the fact that many children keep their mobile phones on constantly means that public space is redefined to invade the child’s home and gives the bully potential access 24 hours a day. Because the child has no place to escape, the sense of intimidation and vulnerability is therefore significantly enhanced.

Furthermore, the possibility of the abusive information being distributed through social networking sites and other platforms means that countless people can have access to the hurtful, abusive or insulting messages being sent, causing the victim a far wider sense of humiliation and exposure. Electronic bullying may therefore be more damaging to children’s emotional development and well-being than traditional bullying. There is a greater power imbalance, with victims sometimes not knowing their bully’s identity, and with the bully having an all-pervasive reach in both space and time.

A Youth Internet Safety Survey conducted in 2005 found that 38 per cent of 10- to 17-year-olds in the United States who experienced cyberbullying reported feeling distressed by the incident. Among the survey respondents, pre-adolescents, those who were victims of aggressive harassment offline (such as receiving telephone calls or being visited at home by the harasser), and those who were harassed by adults were significantly more likely to report being upset. There is also a growing understanding that, like traditional bullying, it can negatively affect the students’ functioning at home and at school, including difficulty with academic performance and emotional distress.

Young people harassed online are more likely than traditional victims of bullying to have social problems, leading to general psychological distress and poor psychosocial adjustment. As a study from the United States found, 31 per cent of victimized students reported being ‘very or extremely upset’, 19 per cent were ‘very or extremely afraid’, and 18 per cent were ‘very or extremely embarrassed’ by online harassment. The study highlighted that cyberbullying contributed to school failure and dropping out, increased depression and anxiety, and in some rare instances led to suicide. A different study found that young people who harass others online are more likely to have problems with breaking rules and aggression.

More recently, a study across 25 countries of the European Union found that, although the actual levels of cyberbullying were low, it is widely experienced as harmful, with only 15 per cent claiming not to have been at all upset by the experience. However, there are considerable variations by gender and socio-economic status: 37 per cent of girls report being ‘very upset’, compared to 23 per cent of boys; and 42 per cent of children from lower socio-economic households said they were very upset when cyberbullied, compared to 22 per cent of those in the high socio-economic group. There is also evidence that cyberbullying, as with traditional forms of bullying, hurts both the victims and bullies, with neither performing well in school because of lower self-esteem, personal insecurities and a heightened sense of paranoia that prevents them from concentrating in the classroom.

Overall, it is clear that cyberbullying is a significant issue in the lives of some young people. While all forms of bullying can be damaging for children, the nature of the experience in cyberspace or via mobile phones increases the potential for harm as it can infiltrate their daily lives without allowing refuge.

**Chapter 5: Sources of support and help**

Children and young people use a range of strategies to protect themselves online. In general, young people report that they usually
turn to an online or offline friend for help, block unwanted messages or change privacy settings. A comparison of representative surveys conducted among children in Ireland, Norway and the United Kingdom found that the frequency of exposure to perceived online risks, especially regarding content, is fairly high, but most children adopt positive strategies to deal with the situation. They may seek help from friends or, more commonly, use neutral strategies such as ignoring the experience. A minority exacerbate the risks through actions such as passing on sexual or violent content to friends.309

The 2011 EU Kids Online study found that 64 per cent of 11- to 16-year-olds said they know how to find safety advice online or how to block messages from those they do not want to contact; 56 per cent are able to change privacy settings themselves and compare websites to judge quality and 51 per cent are able to block spam.310 Research among young people in Bahrain found that the majority of children took action to protect themselves by blocking unwanted approaches or information, or by closing the Web window.311 Overall, they were reluctant to seek adult help, emphasizing a strong preference to keep their Internet activities private.

**KEY MESSAGE**

**Children are less confident about keeping safe in countries where Internet safety information is not widely available.**

According to one survey, Brazilian teenagers’ advice to other young people included declining to add strangers to friend lists, blocking unwanted ‘friends’ and being careful what clothes are worn when opening a webcam.312 The list of advice that South African girls had for their peers, as documented in another survey, included: do not give personal information to anyone you met online, do not send pictures of yourself, tell someone you can trust if somebody threatens you or uses abusive language.313

There seems to be less knowledge on how to keep safe in countries where Internet safety information is not widely available. In a survey of girls and young women in India, for example, those who were aware of incidents of misuse of photos and videos on the Internet reported the incidents among their friends, but barely 10 per cent were aware of the proper authority to report cybercrime.314

**KEY MESSAGE**

Children and young people frequently do not see their parents as the first resource to turn to if they experience online abuse. They often feel their parents do not understand the world in which the abuse arises. Yet evidence from the industrialized world indicates that informed and actively engaged parents who share Internet experiences with their children are the strongest protective factor for ensuring a safer online experience.

Parents are not the primary source of help for many children. Although young people in some countries say they would turn to teachers and parents, others state they would not seek help from these adults because they have even less understanding than young people themselves and therefore would not be in a position to help. In research in Ireland, Norway and the United Kingdom, most strategies adopted by young people tended to exclude adult involvement.315 Across Europe, there may be wide disparities in the numbers of children who would turn to their parents for help. For example, 28 per cent of parents in the Netherlands and 24 per cent of parents in the United Kingdom who participated in the 2008 Eurobarometer survey said that their children asked for help when contacted by a stranger online, found sexually explicit images or were bullied or harassed, compared to only 3 per cent in Bulgaria, Cyprus, Italy and Portugal.316 These differences may correlate with the extent to which their parents are online themselves and therefore have an understanding of the context.

The IYAC global survey supports the findings of other studies by showing that as many as 40 per cent of children do not discuss their activities online with their parents.317 It is worth noting that research conducted among adolescents and youth who experience problems connected with alcohol or drug use or with reproductive health issues also state that they would turn first to their friends before seeking out parents and specialists – adolescence tends to be a developmental
stage that involves exploratory behaviour and pulling away, to a degree, from parents. The lack of primacy given to parents as a source of help may well be consistent with similar patterns associated with other forms of risky behaviour or exposure to potential risk or harm among young people. Whatever parents may wish, some adolescents do not want adults ‘interfering’ in their social space and interactions online. However, additional explanations of why parents are not looked to 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.\textsuperscript{318}

Nevertheless, research also suggests that many children and young people would like parents to be more involved. For example, the IYAC survey cited above also found that 30 per cent of respondents said they spoke openly and regularly with parents and guardians about sites they visited and their concerns.\textsuperscript{318} Children’s exclusion of parents seems not to inevitably derive from reluctance for their support, but rather recognition of limited parental capacity to provide support effectively from the child’s perspective.\textsuperscript{320} Research among girls in Brazil found that they expressed “a clear desire to have parents more involved in monitoring their actions on-line, providing advice and helping them determine what is safe and unsafe.”\textsuperscript{321}

The SaferNet Brasil survey found that 50 per cent of respondents have no parental limits on their Internet access, but almost 52 per cent of those who did have parental limits reported that they accepted such monitoring because they knew that it was for their own safety. The survey also found that 39 per cent of respondents only block and report when they experience some harm or aggression online, 22 per cent ask parents for help, and nearly 14 per cent simply turn off the computer and try to forget what happened. Only 23 per cent identify the family as one of the primary sources for learning more about cyberspace safety, well behind the media, which was cited by 48 per cent of young people as their major source of information about online risks and safety; 21 per cent said that they had never searched for this kind of information.\textsuperscript{322}

Emerging evidence has shed light on effective ways for parents to protect their children. Research from London University’s Institute of Education, for example, asserts that blanket restrictions on Internet use leave children unprepared and unable to protect themselves. Instead, it finds that accurate, comprehensive information and guidance on how to assess and reduce the risks enables children to understand the benefits of the Internet, take a critical view of what they see and browse safely. In other words, parental fears that the Internet will expose children to sexual abuse in social networking sites can result in children not receiving “the information they need to behave safely and sensibly online,” which may lead to ignoring the more frequent dangers of using the Web.\textsuperscript{322} Dialogue and communication seem to provide the best protective environment.

**KEY MESSAGE**

**Messages from an exclusively adult perspective about the need for protection and the nature of risk are likely to fail.**

*Children are unlikely to have a positive response to messages that fail to address or take account of their perspectives. Messages need to be informed by evidence from young people themselves as to the nature of risks and their experience of vulnerability.*

Research by Chang-Hoan Cho and Hongsik John Cheon reveals that it is not simply parents’ Internet knowledge and skill that enables them to positively influence their children’s online activities, but rather it is both the quality and quantity of emotional bonding and shared Web activities.\textsuperscript{324} Parents’ engagement and family cohesion are the keys. The importance of the family is further reinforced in research undertaken by Mia Lorenz and Julia Davidson, which found parental advice to be more effective if there is a close parent-child relationship.\textsuperscript{325} Research findings in the United Kingdom, in 2009, also suggest that young people are more willing to learn about digital technology use via friends, family and trial and error\textsuperscript{326} – again affirming the importance of strong parental support and information-giving in the provision of Internet safety advice.

In various studies, young people report that they would tell the police if there were a serious assault or attack offline. In the United Kingdom research, young people stated that they would also utilize online reporting facilities to seek help.\textsuperscript{327} Respondents to the
Voices of Youth survey in 2010 indicated that they knew the police had access to all sites for surveillance purposes and were aware of such strategies as blocking lists and banning or removing troublesome users. Young people were also familiar with advertising and awareness-raising strategies such as posters, notices, ad campaigns, police talks and training programmes.328

There is limited evidence available as to whether children globally are being provided with consistent, accurate and useful information to inform their online choices. Positive examples of investment by governments to develop such programmes include CEOP’s ‘thinkuknow’ in the United Kingdom, which has been provided throughout schools, reaching up to 7 million schoolchildren aged 5–16.329 ‘Thinkuknow’ is designed to encourage young people to have fun with new technology, while staying in control of the risks. Of course, providing information does not necessarily impact on behaviour. A recent evaluation of ‘thinkuknow’ found that children and young people understand online safety messages, but this may not necessarily change their online behaviour. Particularly for younger children, while the programme did raise their awareness of risks and made them more careful online, the import of the messages tended to fade fairly quickly, with safety advice having little effect on past or planned risk-taking behaviour, including willingness to interact with strangers.330

From the research that does exist, it appears that many countries are not providing information to children on any systematic basis. Recent evidence from Bahrain, a country with high Internet usage, reveals that the majority of children had not received training at school regarding Internet safety, and of the minority that had, provision of such training tended to be ad hoc.331 In the study of 10,000 girls and young women in India, the vast majority had received no guidance or information at all concerning Internet safety.332 Clearly, more work can be done to strengthen outreach programmes that deliver education and training on Internet safety. There is also a need for research to ascertain the most effective means of ensuring that such programmes achieve the goal of enabling young people to make informed choices.
PART TWO:

ONLINE/OFFLINE PROTECTION

The ultimate goal of building a protective online/offline environment for children and young people must be to create the greatest possible opportunity, without discrimination or exclusion, to take advantage of the benefits offered by the online environment, while simultaneously minimizing risks and potential harm in that environment.

Building a protective online/offline environment requires understanding and addressing the ways that children and young people of different ages are at risk to different forms of abuse. As Part One has described, online sexual abuse images mainly involve young children who have little or no power over being abused. In this situation, law enforcement is critical and must mesh with wider child protection services. Combating child abuse images is difficult enough, as Part Two of this report will discuss, but grooming is even more challenging to address.

Grooming is inherently characterized by the power imbalance between adult and child. But it is also necessary to consider the implications of adolescent experimentation, sexuality and drive towards independence as well as their computer expertise. Preventing and responding to grooming needs to include adolescents as well as law enforcement agencies, parents and the ICT industry.

International human rights standards and other legal instruments provide a basic framework. Strategies must be rooted in the realization of human rights for every child – their right to protection from all forms of violence, exploitation and abuse without discrimination; their right to be heard and taken seriously; their right to access to child-friendly and age-appropriate information, to privacy and respect for their evolving capacities; and the obligation to ensure that their best interests are a primary consideration in all legislation, policies and programmes that address the online environment that affects them.

Part Two of this report starts with an overview of key international instruments and commitments. It then makes an assessment of critical challenges facing law enforcement and child protection, and concludes with recommendations for a policy response for building a protective environment.

General recognition of the prevalence and severity of the sexual abuse and exploitation of children, and the need for strengthened legislation to challenge it, only began during the 1990s after the adoption and widespread ratification of the Convention on the Rights of the Child. Since then, there has been consolidation and development of further international human rights standards that address sexual exploitation and abuse. In turn, these have been translated by many governments around the world into national legislation designed to strengthen child protection.

The Convention on the Rights of the Child, however, was drafted well before the emergence of the Internet as a potential environment for abuse and exploitation. Similarly, national legislation, regulations, guidelines, policies and codes of conduct drafted prior to the Internet’s emergence do not take adequate account of the new forms of communication, with its scope, speed and capacity for dissemination, and the consequent opportunities it provides to access and potentially harm children. Nor do such instruments address new crimes such as online grooming or dissemination of manipulated child abuse images.

There is much to be done in both industrialized as well as lower income countries. A comprehensive protection response involves action that
will include 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 of the justice and social welfare sectors. It requires improving the 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 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 and abused through sexual exploitation and abuse via the Internet and to build the capacity of professionals who work with them. In general, this should be within the framework of overarching child protection systems rather than seeking to create ‘new’ services as if these forms of abuse were somehow divorced from that in other contexts.

Given its central role in designing and driving the Internet, the private sector must recognize that intrinsic to expanding access and innovating content is contributing to the wider social goal of making the Internet safer for children and young people. 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. Failure to do this will expose the industry to risk of government 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 risk and how to avoid it 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 support to each other. 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 effective. The active engagement of children 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 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 risk, and parents are in one of the best positions to support them. Parents need to be made aware of the nature of risk and to be 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. Much more coordinated work, however, is needed. In many middle- and low-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 over the Internet knows no borders and coordinated international action by justice and welfare sectors is essential.

**Chapter 6: International instruments and commitments**

Like a number of other child protection issues, the online related abuse and exploitation of children is at the intersection of two sets of international standards, which together 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.

Although there are numerous instruments that contribute generally towards the creation of a protective environment for children,
the five main international and regional legal instruments that are relevant to the sexual exploitation and abuse of children in the online environment are:

- Convention on the Rights of the Child;335
- Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (OPSC);336
- Council of Europe Convention on Cybercrime;338
- Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.339

Not only do these instruments provide guidance in addressing and responding to the sexual exploitation and abuse of children in the online environment, they also establish a set of legally binding obligations for States Parties to these treaties to take specific measures in this respect. Together, they elaborate a comprehensive framework of children’s rights as well as contain specific 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 Optional Protocol to the Convention on the Rights of the Child 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. While the regional instruments only have specific application within the region in which they are developed, they do 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.

Although under international law States have the primary responsibility to ensure respect, promotion and protection of children’s rights, the CRC 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.

In June 2011 the United Nations Human Rights Council endorsed the Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy” Framework. These were developed by the Special Representative of the Secretary-General on human rights and transnational corporations and other business enterprises in six years of research and extensive consultation with governments, companies, business associations, civil society, affected individuals and groups, investors and others.340 The principles provide comprehensive guidance on the obligations of both States and businesses aimed at contributing to enhancing standards and practices with regard to business and human rights.341

They are all relevant to the ICT industry, but Principle 13 (b) is perhaps of particular resonance, stating that the corporate responsibility to respect human rights requires that business enterprises “seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts”.342 In other words, if the private sector provided operations, products, and services that are used to abuse children, businesses have an obligation to take action. The implication of Principle 13 (b) would also be that this includes preventative action if the characteristics of such operations, products and services could be reasonably predicted to carry risk of such abuse.

**Convention on the Rights of the Child**

The Convention on the Rights of the Child, adopted unanimously by the United Nations General Assembly in 1989 and now nearly universally ratified, provides a clear set of entitlements and obligations that must be applied to frame understanding of children’s rights in the context of sexual abuse and exploitation in the online/offline environment. A key element of the Convention is that it
demands that the child be viewed as a holder of a comprehensive set of rights. In other words, States must consider children’s rights holistically. Governments have obligations to take action to ensure the greatest possible safety and protection for all children in every sphere of their lives. In doing so, they must reflect an appropriate balance between the right to protection and the right of children to information, participation, rehabilitation and recovery, privacy and respect for their evolving capacities, and emerging autonomy. Within the context of child protection in a merged online/offline environment, it is worth examining the implications of a number of these rights in more detail.

**General principles**

The Committee on the Rights of the Child has identified four rights in the Convention that also must be understood as general principles to inform the realization of all other rights. All four have relevance to the violence and sexual abuse and exploitation experienced by children in the merged online/offline environment.

Article 2 demands that all the rights in the Convention apply to every child without discrimination on any grounds. Governments must therefore take measures to ensure that the right to protection from sexual exploitation and abuse is addressed in respect to all children, recognizing that the forms of usage, the nature of risks and the degrees of vulnerability will be different for children according to their circumstances – including such factors as gender, social and economic context, rural or urban environment, personal experiences, disability, sexuality, degree of emotional vulnerability or other circumstances that may render them at risk. It is necessary to take into account how different groups of children access the Internet, whether at home, at school, in Internet cafes, and through computers or mobile phones.

Governments must also ensure that primary consideration is given to children’s best interests in all actions concerning them. Article 3 requires that States ensure that in developing legislation, operating law enforcement, and providing social welfare services and other protective measures the best interests of the child remain at the centre of the process. It is a mediating principle that needs to inform the way in which an appropriate balance is achieved, for example, between the policing objective of prosecuting offenders, and the welfare, protection and recovery of the child.

Article 6 requires States to ensure, to the maximum extent possible, the development of the child. Legislation and policies in respect to the online environment therefore must be directed to both promoting the optimum developmental opportunities possible via access to the Internet and ensuring that children’s development is not harmed or hampered by exposure to inappropriate, dangerous or abusive content or contact online.

Finally, article 12 calls upon States to ensure that all children, based on their capabilities, are enabled to express their views freely and to have those views given due weight in accordance with their age and maturity. It also provides that children have the right to be heard in any judicial or administrative proceeding affecting them. In its General Comment on article 12, the Committee on the Rights of the Child makes clear that, in proceedings where a child is a victim of a crime, not only is she or he entitled to be consulted on any matters relevant to the case and on how she or he might be involved in the judicial process, but also to be fully informed about every stage of the process. Furthermore, proceedings must be accessible and child-appropriate, with attention paid to the creation of child-friendly environments. More broadly, it requires that children are consulted on the development of legislation, policy, education and other measures that address all forms of violence.

**Specific protection provisions**

The Convention on the Rights of the Child contains a number of provisions specifically focused on child protection. Article 19, for instance, requires that States take all appropriate legislative, administrative, social and educational measures to protect the child from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse, while in the care of parent(s), legal guardian(s) or any other person(s) who have care of the child. The article does not limit the application of this right to abuses that are the result of state-sanctioned conduct, nor does it narrow its scope to particular manifestations of abuse. As such, there is a positive obligation on the State to protect children from exploitation committed in any space including cyberspace.
The Committee on the Rights of the Child has affirmed the scope of article 19 to address violence through information communication technologies, including the sexual abuse of children in order to produce and disseminate child abuse images, exposure of children to harmful material, bullying, harassment or being groomed for sexual activities. This provision is reinforced by article 34, which requires States to protect the child from all forms of sexual exploitation and sexual abuse. More specifically, the Convention on the Rights of the Child explains that for these purposes, States must take all appropriate national, bilateral and multilateral measures to prevent, among other things, the inducement or coercion of a child to engage in any unlawful sexual activity. No limitations are placed on the terms of engagement. Thus, it implies that if the engagement occurs electronically it too would be a violation of the right; this would include, for example, the offence of Internet grooming.

Additional protection is provided in articles 35 and 36, which require States to take appropriate unilateral, bilateral and multilateral measures to prevent the abduction, sale or trafficking of children, and to protect children against all other forms of harmful exploitation. These provisions introduce obligations to address a broad spectrum of potential abuse in the online environment. States are also required, in article 39, to take all appropriate measures to promote the physical and psychological recovery and social reintegration of a child victim of exploitation and abuse, and to do so in an environment that fosters the health, self-respect and dignity of the child. This provision makes clear that States must go beyond prevention of exploitation and abuse and prosecution of offenders; they also must invest in resources and services to support children who have suffered such abuse.

**Participation provisions**

Article 5 introduces the requirement that guidance given to children by parents or other caregivers must consider the child’s evolving capacities. In other words, as the child gradually acquires the ability to take responsibility for his or her own decisions, then the exercise of rights transfers from the parent to the child. In regard to children’s engagement with the online environment, due consideration needs to be given to:

- The importance of the Internet as a resource and a means of developing and strengthening the capacities of children;
- Recognition of and respect for children’s capacities to make choices and take increasing responsibility for their own protection, in accordance with their evolving capacities;
- Acknowledgement of adults’ responsibilities to remove both harm and impunity from the online environment in view of children’s entitlement to protection as a consequence of their still evolving capacities.

Additionally, children have a right to privacy. Article 16 recognizes the child’s right to freedom from arbitrary interference with his or her privacy, family, home or correspondence. This provision has implications for States to ensure that Internet provider services, and such online access services as social networking sites, online gaming and Internet cafe owners, ensure appropriate levels of privacy for users of these services. It also implies an obligation to ensure that children who are using the Internet have sufficient information and guidance to enable them to protect their own privacy effectively.

Articles 13 and 17 place an obligation on governments to ensure children’s freedom of expression to receive and impart information, regardless of frontiers, through any media of the child’s choice – and to ensure that children have access to information and material from diverse national and international sources. States are also required to encourage the development of guidelines for the protection of children from harmful information and material. Clearly, this provision extends to information and materials in both the online and offline environments.

These human rights norms and standards, together with the international commitments that accompany them, should be applied in a way that provides societies with the framework and goals for building environments in which children’s right to protection from all forms of violence, abuse and exploitation are respected and fulfilled. Simultaneously, the way they are applied should give every child the opportunity to achieve her or his optimum development.
Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (OPSC)

The OPSC, which entered into force in 2002 and was ratified by 149 countries as of September 2011, strengthens the provisions of the Convention on the Rights of the Child in a number of ways relevant to online/offline sexual exploitation. It defines child pornography to include any representation, by any 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, and requires States to criminalize child sexual exploitation offences, whether committed nationally or transnationally. It also requires States to adopt or strengthen, implement and disseminate provisions to prevent sexual offences against children. Of particular relevance to children who are at risk of grooming or other forms of exploitation online is an obligation on States to keep current with new technologies to ensure protection. The Protocol also clarifies that a State must exercise extraterritorial jurisdiction and introduce powers of extradition.

Finally, the OPSC elaborates on governments’ responsibilities to create child-friendly legal proceedings, including protecting the rights of child victims and witnesses without prejudicing the right of the accused to a fair trial; informing child victims of their rights, and of the role and scope, timing and progress of the proceedings; and providing “appropriate support services to child victims,” including the protection of the child’s privacy.

The Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children, supplementing the Convention against Transnational Organized Crime (the UN Trafficking Protocol)

This Protocol came into force in December 2003, and by September 2011 was ratified by 147 States and accepted by the European Community. The UN Trafficking Protocol contains the first detailed and internationally binding definition of ‘trafficking in persons’ and of child trafficking, including for the purpose of sexual exploitation. A child cannot consent to being trafficked: an apparent ‘consent’ is not recognized as a justification for any form of child exploitation. As the Internet has become a means to locate and lure trafficking victims, the application of this Convention and its optional protocols to the merged online/offline environment is significant.

Council of Europe Convention on Cybercrime

The Convention on Cybercrime entered into force in July 2004 and was ratified by 32 States as of September 2011. It is the first international treaty designed to address several categories of crimes committed via the Internet and other computer networks, and binds countries in the same manner as a treaty. The main goal of this convention is to establish a “common criminal policy” to better combat computer-related crimes worldwide by harmonizing national legislation, enhancing law enforcement and judicial capabilities, and improving international cooperation. Although developed by the Council of Europe, the Convention on Cybercrime “increasingly serves as a global guideline for preparation of national legislation as well as a framework for international cooperation against cybercrime, including combating sexual exploitation of children.”

The Convention on Cybercrime defines ‘child pornography’ to include material that visually depicts children or persons appearing to be children engaged in sexually explicit conduct. This is not limited to materials involving a real or identifiable child, but also covers realistic images representing a minor, which may enable the prosecution of pseudo-photographs and computer-manipulated photographs of adults that, for example, make a young adult appear to be a child. Child pornography acts that must be criminalized under this convention include all acts of producing, offering or making available, distributing or transmitting child pornography when these acts are committed through a computer system. It alsocriminalizes the procurement of child pornography through a computer system for oneself or for another person and the possession of child pornography in a computer system or on a computer data storage medium, establishing them as criminal offences when committed intentionally.
Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (the Lanzarote Convention)

The Council of Europe Convention, designed to protect children from sexual exploitation and abuse, was adopted and opened for signature in 2007. It is the first international instrument to tackle all forms of sexual violence against children, including abuse perpetrated within the family environment. Apart from sexual abuse, child prostitution and pornography (child abuse images) and coercing children into participating in pornographic performances, the Lanzarote Convention also deals with grooming and sexual exploitation of children in tourism. It is open for ratification not only by Member States of the Council but also by other States that participated in its elaboration: Canada, the Holy See, Japan, Mexico and the United States. The convention is also open to accession by all other non-member states. Other states can accede to it with unanimous consent of the parties to it (articles 45 and 46). By September 2011, the Convention had been signed by 27 countries and ratified by 15. It came into force on 1 July 2010, following the fifth ratification.349

The aims of this Convention are to prevent and combat the sexual exploitation and abuse of children; to protect the rights of victims of sexual exploitation and sexual abuse; and to promote national and international cooperation against sexual exploitation and sexual abuse of children. It defines child pornography as “any material that visually depicts a child engaged in real or simulated sexually explicit conduct or any depiction of a child’s sexual organs for primarily sexual purposes” (article 20) and encourages State Parties to criminalize child pornography possession, production, offering, making available and procuring, whether for oneself or another person. It further establishes an offence of knowingly obtaining access to child pornography through information and communication technologies, and of corruption of children through intentionally causing them to witness sexual abuse or activities. In addition, it introduces the offence of sexual solicitation of a child for sexual purposes using ICT (grooming), and beyond domestic law, it is the only legal instrument that specifically speaks of grooming.350

In addition to establishing conduct that must be criminalized, the Lanzarote Convention introduces several provisions relating to criminal justice procedures, with particular concern to how they affect victims, based on the principle of the best interests of the child. Safeguards are placed on the victim’s identity and privacy, victim contact with perpetrators is minimized, and intermediaries instead of victims may address courts and present evidence. According to article 31, all information must be given to the victim in a “manner adapted to their age and maturity and in a language that they can understand.” Other provisions mandate that specially trained personnel conduct investigatory and judicial interviews on child-friendly premises (article 35). Finally, it introduces requirements to reduce victim trauma during trial by permitting both closed hearings and the use of appropriate communication technologies for victim testimony and confrontation with the accused.

Commitments by the international community

Since the 1990s, in addition to the core international and regional instruments that strengthen child protection, the United Nations, related bodies and various regional entities have made further commitments and adopted guidelines and codes of conduct designed to strengthen mechanisms for child protection. Progress accelerated with the appointment by the Commission on Human Rights of the Special Rapporteur on the sale of children, child prostitution and child pornography (1990), the Commission’s adoption of a Programme of Action (1992), and the three World 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.

The First World Congress against the Commercial Sexual Exploitation of Children, held in August 1996, was a landmark event, providing testimony that convinced the world that sexual violations against children exist in all nations, irrespective of cultural differences or geographical location. It marked the first public recognition by governments of the existence of commercial sexual exploitation of children and resulted in a global commitment to the ‘Stockholm Declaration and Agenda for Action’, adopted by 122 governments, as a guide to
the specific measures that must be taken to protect children’s right to live free from sexual exploitation.\textsuperscript{351} Since then, a broad alliance of governments and non-government entities has championed this agenda and has made gains in protecting children from commercial sexual exploitation. The increasing sophistication of resources available to those who seek to exploit children, however, has grown in equal measure.

The Second World Congress against the Commercial Sexual Exploitation of Children (December 2001) produced the Yokohama Global Commitment,\textsuperscript{352} which renews States to the Declaration and Agenda for Action established by the first World Congress. It further underscores that national agendas, strategies or plans of action, designated focal points and comprehensive gender-disaggregated data collection must be developed, and that nations must implement child rights-based laws and law enforcement. As information communication technologies were not prevalent at the time of the first World Congress, their emergence had to be specifically addressed in the Yokohama Commitment. It requires States to establish measures to confront the potential dangers of new technologies such as Internet-based child pornography and, simultaneously, to recognize new technologies’ potential for child protection, including from commercial sexual exploitation through dissemination and exchange of information and networking among partners.\textsuperscript{353}

Finally, the World Congress III against the Sexual Exploitation of Children and Adolescents (November 2008) led to the Rio Declaration and Call for Action.\textsuperscript{354} Whereas the Internet was not even mentioned in the Stockholm Declaration and Agenda for Action, it is mentioned 13 times in the Rio Declaration. Specifically, the Rio Declaration calls on States to undertake specific and targeted actions to prevent and stop child abuse images, the use of the Internet and new technologies for the grooming of children for online and offline abuse, and the production and dissemination of child abuse images and other materials. Further, it requires participating governments to conduct educational and awareness-raising campaigns that focus on children, parents, teachers, youth organizations and others working with and for children, with a view to improving their understanding of the risks of sexually exploitative use of the Internet, mobile telephones and other new technologies, including information for children on how to protect themselves, get help and report incidences of child abuse images and online sexual exploitation.

The UN Study on Violence against Children, reported to the General Assembly in 2008, also recognized the need for specific action to enhance the protection of children in the online/offline environment. It recommends that governments:

- “Strengthen efforts to combat the use of information technologies, including the Internet, mobile phones and electronic games, in the sexual exploitation of children and other forms of violence. Support measures to educate and advise children and their carers about the dangers involved in this context. Criminalize and appropriately penalize those who make, distribute, possess or use child pornography.”

- “Encourage the information and communication industry to devise global standards for child protection, undertake research on protective hardware and software solutions, and fund worldwide education campaigns on safe use of the new technologies.”\textsuperscript{355}

The Internet industry today and the complexity of regulation

Fifteen years ago when people spoke about “the Internet industry” it generally meant simply and only Internet Service Providers (ISPs). In each country there tends to be a comparatively small number of them. ISPs continue to have a unique importance because they provide the key gateway to cyberspace. They hold basic information about users’ activities, information which is often essential to law enforcement investigations or other legal processes. However more recently it is other kinds of online service providers, which have come to dominate the Internet value chain.

Today the majority of Internet businesses have only a marginal or no involvement at all in providing primary connectivity. The Internet industry ranges from “Internet giants” such as Facebook and Google through to hundreds of thousands of small businesses, perhaps being run by individuals in their spare time from their garage or the kitchen table. Then there are hardware manufacturers who are producing ever more inventive and interesting ways of going online. Products such as Sony Playstations, the Xbox, Nintendos, Android-based and other forms of smartphones, Apple’s iPhone, iTouch and iPad constitute a major part of the modern ecology of the Internet. Many companies not only make and supply hardware
but are also moving down the value chain to become direct service providers.

The borderless nature of the Internet makes it hard for both national governments and inter-governmental agencies to speak directly to what has now become a highly diffuse and widely dispersed set of interests. One of the key global institutions responsible for the ongoing overall management of the Internet, the Internet Corporation for Assigned Names and Numbers (ICANN), has no direct representation from any government or inter-governmental agency on any of its decision-making bodies, although it does have a Governmental Advisory Committee which provides governments and IGOs with an opportunity to express their views on matters within ICANN’s remit.356

Standards bodies such as the Internet Engineering Taskforce and the World Wide Web Consortium have persons associated with them who work for governmental or quasi-governmental agencies, but the narrow, essentially technical nature of the remits of those bodies limits any scope for influencing a broader policy agenda. For example, the technical standard for delivering location data over the Internet was formulated within the framework of the IETF. This was a development of great social importance and it has obvious implications for child safety. Yet the engineers who developed it regarded that aspect to be beyond their remit.357

Within the industry and among many Internet users there can also be suspicion about the intent behind regulation. The freedom of information and ease of interaction embodied in the Internet are for many users its most important features. These freedoms have had significant social and political impact in many parts of the world, and the Internet has facilitated challenges to those in authority in many places, perhaps most graphically in parts of North Africa and the Middle East during 2011. Inevitably, conservative and authoritarian governments perceive the Internet as something over which they would like more control. However, seeking to impose local and highly restrictive regulation on the Internet would undermine it as a global system and inhibit much of the creativity that it has unleashed. Nevertheless, protecting the vulnerable from exploitation and abuse is necessary. The Internet is not divorced from the morals and responsibilities of the wider world.

For all of these complex and interlocking sets of reasons there is a widespread acknowledgement and acceptance that those private sector enterprises that are actors in the Internet space need to embrace and discharge a wider set of social responsibilities. Around the world this has given rise to a range of self-regulatory and co-regulatory models which are specifically designed to address the interests of children and young people as users of the Internet. Some countries, such as the United Kingdom, have adopted a position of allowing the ICT industry to self-regulate. Other governments, such as the United States, have not taken a formal public position on the issue, instead relying on the ‘corporate social responsibility’ model to motivate businesses to protect children.

That the industry steps up to the mark on child safety and protection is in its interests. Failure to act promptly and with leadership on legitimate protection concerns, ones that States are legally obliged under international law to ensure are addressed, risks governments or regional bodies legislating to compel compliance to restrictive laws within their jurisdiction. To some extent this is already happening. A number of countries have introduced national laws and regulations which they feel suit their cultural, legal and political traditions. However, many more governments have refrained from such action in the belief that a co-operative approach will be better for everyone. But should faith in cooperation be shown to be fruitless, a proliferation of new national or regional laws and regulations could be expected which would truly fracture the idea of a single global system or a single global network.

Despite examples of socially responsible practice, the lack of a single point of accountability or reference has at times spilled over into evident frustration at a perceived lack of responsiveness to what governments or independent bodies discharged with protecting privacy feel are their legitimate concerns. The final communiqué of the 2011 G8 meeting made express references to the position of children as Internet users and as potential victims of trafficking or sexual abuse and exploitation mediated through the Internet. It included a call for enhanced cooperation within and between all international fora dealing with the governance of the Internet.358
Multinational approaches contributing to the protection of children online

In 2008 the International Telecommunications Union (ITU), the United Nations specialized agency for information and communication technologies, launched the Child Online Protection initiative (COP), bringing together a broad spectrum of governmental and intergovernmental agencies, law enforcement agencies, industry and civil society representatives. These disparate interests collaborated with ITU officials to promote a set of documents which present a series of recommendations to policy-makers, to children, industry, parents, guardians and educators.359

In 2010 the ITU commissioned a survey of national governments where it asked them to describe what they thought the major issues were with online child protection in their country and what help they thought they needed in this area.360 In November, 2010, the ITU published the Child Online Protection Statistical Framework, presenting it as the “world’s first attempt to provide the overall statistical framework related to the measurement of child online protection with a particular emphasis on measures that are suitable for international comparison”.361

The ITU continues to attach a high priority to its work on online child protection. It is particularly active through regional seminars in all parts of the world. Internally, the security standardization study group, Study Group 17, was tasked in March 2011 to investigate child protection in the online world with a view to determining what scope there is for developing technical standards which can be offered for adoption.362

Also within the framework of the UN, the Internet Governance Forum (IGF) provides a forum for multi-stakeholder policy dialogue. It attracts high level participation from global, regional and national industry groups. Child protection issues have become a regular feature at its annual congress and at many of the regional IGFs which have sprung up on all continents. For example, the protection of children was discussed at plenaries in the IGF meeting in Hyderabad in 2008 and at Sharm el Sheikh in 2009.363

European Union initiatives

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.364

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.365

Prior to the 2004 Framework Decision, the European Commission established the Safer Internet Programme in 1999, with a particular emphasis on protecting children and the objectives of promoting safer use of the Internet and other communication technologies, educating users and fighting against illegal content. The current programme spans 2009–2013 and has a budget of €55 million; its original remit has been expanded to cover emerging online technologies and harmful conduct such as grooming and cyberbullying.366

The EU was an early champion of self-regulation to keep young people safe online. In February 2007, leading mobile operators and content providers across the EU signed a European Framework for safer mobile use by children and teenagers. As of June 2010, codes of conduct were in place in 25 EU member States, while under development in the remaining two. 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 codes of conduct.367

Two years after the adoption of the code on the safer use of mobile phones, in February, 2009, 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 activities and reporting abuse functions. The social networking principles have now been subject to a second appraisal, published in May 2011. Here the findings were more mixed, with the responses of 4 of the 14 SNS that replied to the survey about explicit information regarding the characteristics (e.g. age-appropriateness, availability, user-friendliness, etc.) of privacy settings assessed as unsatisfactory.368

In June 2011, the European Commission held its first Digital Assembly Agenda. 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 when the text will be released.

Other regional initiatives

Although there are presently no inter-American protocols or instruments specific to the protection of children in the online/offline environment, relevant regional materials do exist. The Inter-American Children’s Institute, based in Uruguay, has presented numerous reports on the commercial sexual exploitation of children, and the Memorandum of Montevideo, developed in July 2009 by a group of experts, provides a framework for protecting children’s personal information in cyberspace.369 Designed to guide legislators, judges, policymakers, and law-enforcement officers on how to protect children’s personal data online, the Memorandum of Montevideo provides recommendations concerning prevention and education, legal frameworks, law enforcement and public policy.370 It emphasizes prevention through education, stressing that children learn about the positive and negative aspects of using a pseudonym as well as the risks associated with Internet usage; recommends establishing simple, speedy and easily accessible judicial processes based on tort law; and advocates for publishing case law related to Internet offences and the establishment of response mechanisms for assisting the victims of abuse in cyberspace.371 Although the Memorandum is not binding on any Latin American national government, it acts as an important framework for countries that are seeking to protect children’s personal information online.

Chapter 7: Challenges for law enforcement and child protection

International treaties and other commitments provide the framework for action, but governments must translate these into action at the national level. This requires policy development, preventive strategies (including the involvement of civil society, parents and children), appropriate laws, effective policing strategies, child protection measures and response services for child victims.

The new environment poses profoundly different challenges for law enforcement and child welfare agencies, given the international dimension of much of the abuse, its hidden nature, and the speed of both the adoption of new social applications by young people and technological advances that offenders are able to exploit to evade prosecution.

During recent years, new approaches have been developed on the international, regional and national levels to provide such protection. New ‘architecture’ to facilitate the successful pursuit and prosecution of offenders has been created. These include the definition of new crimes and penalties, partnerships with credit card companies to track offenders, bilateral and international collaborations, shared databases, and measures to address jurisdiction and extradition. A key point is that police and protection services must work closely together to resolve sometimes differing imperatives in the child’s best interests.

National legislation

Despite the increased focus on sexual exploitation and abuse of children at the
international level, and the development of new global and regional human rights instruments, many nations have been woefully slow in implementing necessary legislation. A number of recent global reviews provide testimony to the limitations of progress to date.

A common theme across the background reports on child abuse images for all three World Congresses was the need to harmonize relevant laws. While reviewing State Party reports, the Committee on the Rights of the Child has consistently noted the need for clear definitions and has recommended that States amend existing legislation or adopt new legislation to bring them in line with the OPSC. The Committee has identified weak legislation, as demonstrated by low rates of identification and prosecution of cases, and has highlighted the difficulties in extraditing and prosecuting crimes committed outside a State’s territory due to the requirement in many countries for ‘dual criminality’, or extraterritorial legislation that requires an act to be a crime in both the country where it took place and the country where the suspect resides. The Committee systematically recommends abolishing this requirement.

Najat M’jid Maalla, the Special Rapporteur on the sale of children, child prostitution and child pornography, expressed continuing concern in her 2009 report that not only do some countries lack any legislation covering child abuse images but, even where such laws exist, significant differences in national responses to the phenomenon remain. ECPAT International, working collaboratively with other partners, has produced 77 country reports that seek to provide a baseline of information on actions taken and the remaining gaps for addressing sexual exploitation of children in each country. A common foreword to the reports notes that government “actions have not been uniform and, as these country profiles attest, far more urgent work must be done to protect children from such heinous violations, as these are still perpetrated with impunity in many countries.”

The age at which a person can consent to sexual activity also varies from country to country, presenting a significant challenge to the consistent and harmonized protection of children from sexual exploitation on the international level.

To gain a better understanding of existing legislation and to gauge where the issue stands on national political agendas, the International Centre for Missing & Exploited Children provides ongoing reviews of child pornography legislation. The Centre focuses its evaluation on whether national legislation:

- Exists with specific regard to child pornography;
- Provides a definition of child pornography;
- Criminalizes computer-facilitated offences;
- Criminalizes possession of child pornography, regardless of the intent to distribute;
- Requires Internet service providers (ISPs) to report suspected child pornography to law enforcement or another mandated agency.

The results are not encouraging. In 2010, of the 196 countries reviewed, 45 have legislation sufficient to combat child abuse image offences and 89 had no legislation at all that specifically addresses child pornography. Among the 45 countries that have sufficient legislation, 37 meet all but the last criteria, relating to ISP reporting, and just 8 meet all the criteria. Of the countries that have legislation, 52 do not define child pornography in 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.

In 2009, the group of eight industrialized countries known as the G8 reaffirmed its commitment to tackling child pornography in the declaration ‘The Risk to Children Posed by Child Pornography Offenders’, which emphasized the need for international cooperation and noted that some countries had not adopted effective legislation to criminalize child pornography. The G8 has supported several important initiatives recently, including the ‘G8 Wanted Child Sex Offender Initiative’ website hosted by INTERPOL, a report on international sexually motivated child abduction, and a current project led by Japan that examines international efforts to support child victims of sexual exploitation and abuse and will make recommendations as to best practice in this area.

In addition to legislation on child pornography, Australia, Canada, Singapore, the United Kingdom and the United States have introduced legal measures to deal with offences related to online child grooming. The Australian and Canadian legislation criminalizes electronic communication with a child or a person believed to be a child for the purpose of
facilitating the commission of sexual offence. This, in effect, means that even when a suspect of a grooming offence establishes contact with an adult pretending to be a child, as in cases of undercover police investigations, there is no impediment to a prosecution.381

Brazil’s Statute of the Child and Adolescent382 was amended in 2008 to address online sexual abuse of children. As noted by the US Law Library of Congress, the modifications penalize “the enticement, harassment, instigation, or constraint, by any means of communication, of a child, with the purpose of practicing with the child lustful acts.” Punishment is also defined for those who facilitate or induce “the access of a child to material containing an explicit sex or pornographic scene” and for “inducing the child to expose herself in a pornographic or sexually explicit way.”383

In the United Kingdom, the Sexual Offences Act of 2003 established the legal framework to protect children from sexual exploitation, including Internet child pornography and grooming. Noteworthy elements of this act include the absolute prohibition of sexual activities with a child under age 13 and that no child under 13 can legally give consent. Sexual activity with a child includes intercourse, sexual touching, encouraging a child to engage in sexual acts with someone else, or forcing a child to strip or masturbate, even if the intended activity does not take place. If an offender is over 18 years old and has communicated with a child under 16 at least twice, including via a phone or the Internet, it is an offence to meet or travel to meet the child, anywhere in the world, with the intention of committing one of the offences listed in the law.384

Japan has passed a series of laws to protect children in cyberspace. The Act on Punishment of Activities Relating to Child Prostitution and Pornography and the Protection of Children,385 originally passed in 1999, was designed to reduce the prevalence of child abuse images and child prostitution and to protect children from sexual exploitation and abuse. It was revised in 2004 to increase the statutory penalties for these crimes. A 2008 attempt to amend the act to criminalize the “simple possession of child pornography” has yet to be enacted.386 Two additional laws that deal specifically with the online environment are the 2003 Online Dating Site Regulation Law387 and the 2008 Act on Development of an Environment that Provides Safe and Secure Internet Use for Young People.388 In addition to these laws, the Cabinet Office together with 9 ministries and agencies, including the National Police Agency and the Internet Affairs and Communications Ministry, introduced general measures to eliminate child abuse images and establish a council with representation from the private sector and civil society organizations to raise public awareness.

Law enforcement and child protection

Legislation and political commitments, while of fundamental importance, cannot achieve change unless there are mechanisms in place to implement and enforce them. Law enforcement agencies charged with the responsibility for ensuring that laws are applied consistently and effectively and that offenders are prosecuted and held to account, have vital roles in challenging sexual exploitation and abuse of children in the merged online/ offline environment. And they must collaborate with the social welfare agencies that have a responsibility to promote and protect the best interests of children who have experienced abuse. Their two agendas, however, can sometimes come into conflict. The challenge is to explore approaches that are both effective at bringing successful prosecutions while ensuring that the interests of the individual children concerned remain paramount.

The online environment of the 21st century has transformed criminality in a number of ways. The Internet is an advanced vehicle for communication; it has created a transnational environment that provides new opportunities for harmful activities; and, finally, the virtual nature of the online environment means criminal activity can sometimes fall outside the jurisdiction of the criminal justice process.389 The advances in information and communication technologies have created different demands on law enforcement agencies in tackling abuse. They necessitate different and innovative approaches to policing, requiring investigators to negotiate new barriers and technologies, and often to enforce and apply laws in the merged online/ offline sphere that were designed only for the offline environment.390

Cyberspace also introduces new challenges in terms of the nature and scale of the crimes that are being committed against children, as
well as the sheer numbers of perpetrators. The challenges are compounded by the facts that online crimes require few resources relative to the potential damage caused, and they can be committed in a jurisdiction in which the criminal is not physically present. As noted in a 2009 report by the Kids’ Internet Safety Alliance, the Internet has created a crime environment in which there is an imbalance between “the capacity of offenders to offend, and the capacity of law enforcement agencies to respond.” Finally, crimes committed against children in the online environment pose new challenges in relationship to rights to privacy and anonymity, as well as in balancing the prosecution of offenders with the best interests of the child who is a victim of their crime.

Inadequate understanding at the policy level of the implications of child agency and risk-taking behaviours

Globally, despite a growing body of evidence relating to children’s online behaviours, there is insufficient application of this learning to policymaking responses. Interventions set in place to tackle the abuse of children in social networking sites, for example, have sometimes been based on an inadequate understanding of the complexities of the phenomenon. Quick-fix interventions designed to protect children by limiting their access to the Internet may result in harmful unintended consequences for young people.

Flawed legislation quickly becomes irrelevant in the face of technological developments. In the developing world, Internet expansion will likely be through mobile technology, so there too, filtering in schools or libraries would not be an effective protection strategy. The key message of most research so far is that it is behaviour – not technology – that puts young people at risk. As concluded by a consultation with young people and other key stakeholders in the United Kingdom, in 2006, the range of safeguards that had been established at that time were “overbroad and under-specific, based on a less-than-complete understanding of the complexities of this phenomenon. Consequently, these interventions have not had a visible impact on the risks faced by young social network users, perceptions of the prevalence of these risks, or dissuaded youth from engaging in online behaviours that can put them at risk of harm.”

A borderless crime

The Internet has been described as borderless because it can be accessed by anyone with a network connection, regardless of location. Crime prevention may no longer be about surveillance and investigation within the immediate community but instead can cross local, national and international geographical boundaries. It may not always be easy to assign a jurisdiction to a crime committed in the virtual environment. Particular crimes might also involve many victims from different countries thus complicating processes even further. Crimes of online sexual abuse and exploitation might involve offenders who are planning them in locations thousands of miles away.

These factors lead to significant challenges for law enforcement. An effective response requires greater collaboration between police forces in different countries – spanning very different jurisdictional protocols as well as social and cultural environments, political expectations, and levels of capacity, technical expertise and resources. Even in the most affluent nations, resourcing is a problem, with police unable to afford many transnational investigations. Further, legal instruments for seizing evidence abroad are often unwieldy and cumbersome. Some countries have introduced legal instruments that seek to address the extra-territorial prosecution of their own citizens who commit offences, such as the United Kingdom’s Sexual Offences Act of 2003. But the solutions are complicated by the fact that what is illegal in one country could be legal in another. For example, only two countries in Africa have legislation deemed sufficient to combat child pornography, the age of consent to sexual activity varies widely across Europe, and online grooming is not universally criminalized.

Determining when a crime has been committed

Establishing that a crime of sexually exploiting or abusing a child online has occurred is not a straightforward process. A unique characteristic of the online environment is that physical contact between the child and the offender does not need to occur for a child to become a victim or for a crime to be committed. The challenges for law enforcement agencies are particularly great when the law does not provide clear definitions of criminal activity in regard to online sexual exploitation of children. Such necessary definitions include whether
‘intent’ to lure a child is a crime without actual contact being made; what evidence of ‘intent’ is required; what constitutes a ‘pornographic’ image of a child; or whether simulated images of children engaged in sexual behaviour are criminalized.

In regard to grooming, for example, article 23 of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse outlines the obligations of States regarding “solicitation of children for sexual purposes.” Countries that are party to the convention have agreed to criminalize any intentional proposal made through information and communication technologies by an adult to meet with a child – as defined by national law – for the purposes of engaging in sexual activities or producing child pornography when “this proposal has been followed by material acts leading to such a meeting.”

To address the fact that grooming may not be followed by ‘material acts’, a number of jurisdictions have introduced legislation to criminalize intent when plans have been made to meet a child, even when no physical meeting has taken place. In the United Kingdom, for instance, section 15 of the Sexual Offences Act 2003 introduces three components to the crime of grooming: (1) there must be communication on at least two occasions; (2) those communications must contain evidence of an illegal sexual intent linked to arranging to meet; (3) the person has to have travelled or begun travelling to the meeting. It is not necessary, however, for actual contact to have been made. This definition of the ‘grooming’ offence is designed to protect children before they come into any physical or sexual contact with the abuser.

A noteworthy interpretation of intent was made by Canada’s Supreme Court in 2005. The case involved a man who presented himself as a 17-year-old and conducted two private online chats consisting of sexually explicit conversation with a 12-year-old girl who claimed to be 13. The man persuaded the girl to give him her telephone number and he called her twice in order to ‘talk dirty’ to her. During the second call, he told her he wanted to perform a certain sexual act upon her at which point she hung up. They had no further contact. The child’s father subsequently found out and contacted the police. The man’s computer was seized and he was charged with luring a child. His defence was that he simply was engaging in talking with the 12-year-old and nothing else; he had made no attempt to meet her and had no intention of meeting her. The trial judge found him ‘not guilty’ because there was insufficient evidence that he had intended to lure the girl in order to commit an offence of sexual touching. The prosecution appealed, and the case ultimately went to the Supreme Court, which found that it was not necessary for the offender to meet or even intend to meet the victim in order to be found guilty of luring. Essentially, in cases where the accused and the victim have never met, the Supreme Court has eliminated the defence that the accused had no intention of actually committing a sexual offence with the child and was merely having a conversation.

**Barriers to effective reporting**

Sexual abuse and exploitation in the merged online/offline environment are characterized by their hidden, unreported and under-recorded nature. In order for the police to respond to abuse, they first need a report that an offence has been committed. In the context of online exploitation, this can be challenging. Research indicates that children who are the subjects of child abuse images via new technologies are often afraid to speak about the abuse. As noted by Tink Palmer: “Children who have been sexually abused seldom disclose their abuse. For children who are the victims of abusive images disclosure is even harder.”

The process of silencing children is achieved by the abuser’s actions to make the child feel complicit in the activity. Many victims of abusive images believe that the caring adults around them, as well as the viewers of abusive images, see them as willing participants and therefore in some way culpable. This makes it extremely difficult for them to tell anyone what is happening or has happened to them. Most sexual abuse of children goes undisclosed. When that abuse takes place online, the level of disclosure is even lower.

Because of feelings of shame and complicity, many victims of Internet crime do not disclose their victimization until the pictures or images are most typically discovered by law enforcement agencies during an investigation. In one sample of 14 children referred for therapeutic help in the United Kingdom, it was found that none had reported the abuse. It was only discovered when: (a) police found images while carrying out forensic examinations of computers and mobile phones of suspects who had raped women they had met online and when the women had reported the rape; or (b) close family members noted a change in the
well-being and behaviour of the young people and suspected that something had happened via their online activity. All the children stressed that they would never have told anybody about their abuse if it hadn’t been discovered by some other means. The reasons for this reluctance to report included the highly sexual nature of the language that the young people had used, the ‘complicity’ that they felt because they had often themselves been suggestive in language and willingness to be involved in sexual activity, and the fact that they had lied about their age.404

The degree of anxiety children experience in regard to exposure can mean that even when it is absolutely clear to investigating officers that a child they are interviewing features in discovered images, the child will still deny it is them.405

Some children who have been abused perceive the persons they have formed a relationship with online as their boyfriends, whom they love and upon whom they are emotionally dependent. Some children who are vulnerable to grooming may be less supported socially, more isolated and less likely to report victimization to law enforcement. Furthermore, many children do not realize that they have been victims of a crime because innocent images of children can be digitally transformed into pornographic material and distributed across the Internet without the victims’ knowledge.406

Finally, some reports are made by the private sector, such as moderators of chat rooms. The private sector, however, needs a specific point of contact in a law enforcement agency in order to make a report, without which it may not be referred to the correct department. The question of who receives the report within the police is crucial, and effective routes of referral are essential to a good response.407

Promoting the best interests of the child

In any investigation of online sexual exploitation or abuse, consistent with obligations of the State Party under the Convention on the Rights of the Child, the best interests of the child must be a primary consideration. Law enforcement agencies often need children who have been victims of crimes to be able to serve as credible witnesses in court. The challenge is that investigations and cross-examinations can in themselves effectively involve re-victimization of children, while requirements of courts in criminal proceedings may lead to children being denied therapeutic help pending the hearings. It is important for these issues to be given appropriate priority in policing and prosecution strategies. One effective way of doing this is to build cross-sectoral teams involving police and social welfare officers from the outset of the investigation. (See box 3: Holistic and child-centred investigations, page 82.)

Victim identification

A stronger focus on the child as a victim requires redoubling efforts to identify the children whose images of abuse have been posted online so they can be protected and offered appropriate psychosocial support and rehabilitation. This poses huge challenges. Images on the Internet can circulate for many years. Therefore, a picture of a 5-year-old girl may be 20 years out of date. Interpol 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 a collection can be found in other images within the database, and whether other images of the child at a different age are contained in the database. The police identify a picture of a 5-year-old child, for example, and the database provides information of that child already documented in the database at age 8–10. The police can then focus their energies on looking for an older child.

Although databases of victim photographs do serve as valuable resources, until recently, they have necessitated repeated viewings of those images. As observed by the United Nations Special Rapporteur on the sale of children, child prostitution and child pornography: “While image banks have proven useful, the consequences of storing and exchange of images for the victims must not be ignored. Victims do not necessarily draw a distinction between the persons looking at their images or the reasons they are looking at them.”408 In other words, as far as the victim is concerned, the image continues to be in circulation. Although the United Nations Special Rapporteur was not suggesting that image databases should not be used, she was highlighting 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.

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 the police needing to view the actual image. Typically, only when a new hash is identified is it necessary to produce or look at the image to check its content. In this way, the child's privacy is protected, and the painful experience of knowing that even the route to protection involves further exposure is, to an extent, avoided.

There are, nonetheless, continuing issues regarding image analysis and victim identification processes, including:

- Computer-assisted victim identification is a highly specialized and rigorous process, requiring time, expertise and cutting-edge computer technology. Few, if any, developing countries are likely to be able to afford it.

- Technology only provides part of the solution. Because victim identification is exceptionally detailed work that involves examining the slightest of clues, many aspects of the analysis must be undertaken by human investigators.

- The success rate remains relatively low. In 2009, for example, the INTERPOL Child Abuse Image Database contained more than 550,000 images; from this database, 870 children were identified and rescued.

Another ethical dilemma is whether individuals who are now adults should be identified. It could be argued that whenever a serious crime has been detected it should be investigated, and that identifying and contacting a victim, even as an adult, could prevent future abuse. The victim may be able to lead the police to the abuser, who may still have access to children. Nevertheless, the issue is controversial.

Maxwell Taylor and Ethel Quayle, for example, have questioned the legitimacy of such contacts. They argue that some victims may not know they had been photographed or that the images were in circulation until they were contacted by the police. In other cases, they may have hidden the abuse from their family, are afraid of being held complicit in the abuse images or have resolved their feelings about the past. In all of these instances, police contact could result in significant trauma. On the other hand, it is possible that an approach from the police would be welcomed, particularly if it belatedly offered the chance to prosecute the offender. Law enforcement agencies, of course, cannot know the victim's response until they have made contact. There is no easy solution to this problem, but it needs careful consideration by law enforcement agencies, along with appropriate guidance and training for those engaged in this work.

Dealing with disclosure

The challenge of disclosure is 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, the perpetrator and others who are important people in their lives. By telling, the ‘nightmare’ becomes a reality. Thus children are not only affected by the abuse itself, but may also be traumatized by the disclosure or the consequences of disclosure.

This has particular significance for children groomed online and made the subjects of abusive images; in the majority of such cases, it is the professionals who make the initial disclosure to the child rather than the other way around. The handling of this initial engagement is critical. Without sensitive management to enable the child to trust the professional, the victim may close down emotionally and retreat into denial. Many child victims will deny the abuse even when confronted with the images. They will often minimize any knowledge of being harmed and will remain silent on the matter. When questioned, some victims only provide information that they think the interviewer already knows. Once the child closes down, providing therapeutic help to the child becomes more difficult, and the opportunity to identify and pursue the offender is jeopardized.

Anonymity

The Internet is commonly perceived to offer users anonymity, enabling them to construct identities and determine when, how and to what extent information about them is communicated to others in the online environment. By so doing, their personal identity or personally identifiable information is not known, and the presumed anonymity of Internet activities creates a sense of security and secrecy for both the offender and the victim. This, of course, includes potential offenders. As described by a report in 2009, “relative anonymity enables individuals to behave in ways that they would consider to be unthinkable in the physical world.” Traditionally, in order to find their
victims in an offline context, child sex offenders needed to stalk public places where children tended to gather, such as school playgrounds or social clubs. Today, the high level of social interaction by children online provides offenders with a new environment to target children, in which the risks that they previously faced when making contact in person are apparently eliminated.

Once individuals use the Internet, however, they typically leave a ‘digital trail’, or electronic footprint, that offers new tools for police investigations of child sex crimes and allows law enforcement agencies to collect valuable forensic evidence. The head of intelligence at the Child Exploitation and Online Protection (CEOP) Centre, for example, has stated: “The anonymity that the Internet offers is simply an illusion and we will continue to use technology against offenders and track their digital footprint to hold them to account in order to protect children from abuse.”

A user’s footprint is created through an Internet Protocol (IP) address that identifies a computer on a network. Every computer connected to the Internet requires an IP address to ensure that data moves back and forth through the network to the correct destinations. An IP address is therefore a unique, digital signature and can be correlated with specific subscriber details. In operations where a server has been seized, it is possible to extract information pertaining to each IP address from which images were accessed, which can lead to determining the identity of the individual behind it. This frequently identifies thousands of suspect IP addresses.

Legislation providing authorization to release the identity of the individual behind the IP address will necessarily vary across different jurisdictions. To date in the United Kingdom, for example, ISPs have failed to retain the necessary data in as many as 50 per cent of all cases. CEOP has led operations in which thousands of IP addresses were identified, but many could not be resolved without subscriber data. Privacy advocates and service providers defend their reluctance to retain data on grounds that it is costly and unnecessary because very little of this data is ever used by law enforcement, and that retaining such large volumes of data is a major security risk. This problem should have been addressed in the EU at least, as a 2006 directive requires ISPs to retain data for up to six months and not longer than two years.

There is evidence that offenders are becoming more sophisticated in their strategies to avoid detection. One of the most important tactics is changing their choice of technology. For example, law enforcement agencies have noted an increase in the use of “anonymising” services. At the turn of the century, Web- or newsgroup-based circulation of images was the primary method of distribution. Recent analysis suggests that peer-to-peer distribution, which avoids the necessity of housing the images on machines owned by third parties such as Internet service providers, is now a major form of image distribution. Increasingly within peer-to-peer and other environments, encryption techniques are used, which offer further security to the offender. This phenomenon is likely to grow as such programmes become easier to use and computer-processing speeds make them quicker to process.

The growth of wireless technology has also created a new opportunity for offenders to evade detection. An unsecured wireless connection allows anyone to gain access to it, and if illegal material is downloaded, it will be traced to the owner of the wireless connection and not the user. Criminal justice agencies are warning the public to encrypt their wireless connections to avoid being an unsuspecting conduit for illegal online activities. Additionally, ‘pay and go’ wireless services that do not require registration allow offenders to remain anonymous. With prepaid wireless cards, no forensic evidence can be linked to the offender. Prepaid wireless services are more attractive than cybercafes, where offenders risk their activities being viewed by others.

Law enforcement agencies are caught in a constant game of catch-up, as offenders explore more creative means of evading the law and the police develop new techniques, programmes and partnerships to overcome these evasions. Collaboration across jurisdictions and with the private sector (such as Internet service providers willing to provide police with IP addresses) is critical in supporting the role of law enforcement. This opportunity is strengthened by the Council of Europe Convention on Cybercrime, in article 18, which gives law enforcement authorities the power to compel service providers to monitor a person’s online activities.

**Police capabilities**

Investigations into online criminal activity are complex and time-consuming, often involving coordination across different jurisdictions and
concerning a huge network of offenders. This poses a number of challenges.

The first challenge is limited specialist expertise. Tackling online/offline child sexual abuse and exploitation requires combined expertise in policing, computer and Internet technology, and child protection. There is a distinction between computer crime and computer-related crime. Investigators in both types of crime need training in specialized sets of skills. Information on computer crimes is usually stored on the computer, requiring technical knowledge to retrieve any incriminating evidence, while computer-related crimes, such as grooming, require information from the victim. The ability to present such data in court requires additional skills.

Effective work with online/offline abuse and exploitation demands the acquisition, development and retention of specialist staff. But in many developing countries, specialist units are largely absent, meaning that staff are unlikely to have the necessary training to investigate online crime. And even if they do have the skills, the technology to investigate the crime may not be available. Consequently, many law enforcement officers are at a disadvantage in detecting, investigating and prosecuting online crime. The problem is compounded by the speed of change in technology and by offenders’ abilities to exploit new developments in access to children and in strategies for evading identification.424

Another challenge is the lack of multi-agency approaches. Law enforcement agencies do not always view online sexual exploitation as a child protection issue. Rather, in many countries, online/offline child sexual exploitation is regarded as ‘cybercrime’. E-crime or cybercrime police departments are often focused on fraud and organized crime and may therefore have little or no expertise, or professional interest, in child protection. While organized 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 sex abuse image exchange and grooming does not. Grooming is not perpetrated by organized criminals in the traditional sense and is more commonplace than organized, commercial child abuse image distribution. Thus, cybercrime departments do not prioritize grooming and many cases are not pursued. The categorization of online child sexual exploitation as cybercrime misrepresents the nature of the offending. It also excludes child protection specialists, who are essential throughout the process. Police need to deliver a child-centred response, which rarely happens when they investigate on their own. Child protection specialists ensure that the child is adequately safeguarded and the child’s welfare is taken into account at each stage of the investigation.425

A third obstacle is the status of child protection work. In many police forces, building expertise in the field of child protection is viewed as low-status work with limited career prospects, rendering it difficult to recruit high-calibre personnel. A number of countries – including Australia, New Zealand, the United Kingdom and the United States – have responded by establishing specialist units that develop expertise in sexual exploitation and abuse online and utilize the expertise and experience of trained officers effectively.426 In 2003 law enforcement agencies from Australia, the United Kingdom and the United States, along with Canada and INTERPOL, formed the Virtual Global Taskforce to develop a 24-7 online capability to respond to online incidents. Since its foundation, police services from Europol, Italy, New Zealand, and the United Arab Emirates have become members.427

The complexity of gathering evidence is also challenging. Both the nature of evidence required and the sources of that evidence will differ in the online and offline environments. Successful investigations must access information from both. To be effective, however, investigators who examine the electronic crime scene need to know how to handle, collate and store admissible computer evidence.428 In the online environment investigators need to examine the number of screen names used by the offender; know whether there is a screen profile that suggests deviant behaviour; see whether there is a photograph; and, even more importantly, ascertain whether the profile is accurate in terms of age or gender. Other considerations in relation to online behaviour include how long the offender has had access to the Internet, when and how much time the individual has spent online, how many people have communicated with the offender and how many were regular contacts. Investigators also need to examine the offender’s activities in the physical world, such as their employment, access to young children through volunteering or other activities, and their record of travel. The police gathering this evidence must know where to look, may have to prove the identity of the offender and victim, coordinate investigative activities, and enhance the
Child Safety Online

exchange of information and intelligence between different agencies.

Finally, forensic capability is also a challenge. The scale of offending behaviour in relation to online abuse of children has grown exponentially during recent years, placing major demands on police time. Real-time abuse creates volumes of new abusive images. The growing capacity of computer hard drives to store increasing amounts of data means that the investigative process of online sexual abuse can be extensive and protracted. The extraction and analysis of the offending files, video clips and Internet cache from just one computer can take days, involving the analysis of the correspondence, uploads and downloads in the chat room used to distribute abusive images. Media storage has grown even further in size and sophistication. The amount of data that can be seized by the police is almost incomprehensible. It could take one officer the whole of his working career to thoroughly investigate the contents of a 10-gigabyte hard drive.

Lack of capacity among professionals working with children

There is limited evidence on how social welfare professionals are responding to the new challenges of child protection in the online/offline environment. In general, professionals who come into contact with children – schoolteachers, nursery and school nurses, health personnel, police officers, social workers, counsellors and psychotherapists – are not sufficiently aware of the issues regarding abuse via the new technologies. If, for example, they were concerned about changes in a 13-year-olds’ behaviour, they may not consider that the child might be the victim of online abusive behaviour and therefore don’t ask the child about his or her online life. Furthermore, they are not always prepared or able to hear what children want to tell them. The causes of such gaps range from 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 ICT is progressively becoming more central to the lives of increasing numbers of children across the world, this lack of awareness means that some professionals are failing to pick up on an increasingly important context for abuse.

This lack of awareness is well illustrated in two recent reports, and although they both come from northern Europe, it is likely that they reflect the global picture. In the first study, professionals were interviewed from all the specialized institutions in Germany that offer recovery services to children who had been sexually abused. The authors’ objectives were to ascertain how many of the children with whom these professionals worked were subjects of abusive images, and to raise awareness of the needs of this particular cohort of children. The professionals recognized, in hindsight, that they had failed to respond to or correctly interpret victims’ hints to them. The professionals were simply not sensitized to the risks of Internet abuse. The research highlighted the need for children to feel confident that the social worker or counsellor was aware of the issue of child abuse images as well as the importance of building trusting relationships and being patient. It was clear, however, that the professionals lacked the knowledge on how to identify, approach and help such children.

Similar conclusions were reached in a 2010 study carried out in Norway. The purpose of the research was to find out what child protective service workers knew about harmful online behaviours and how they incorporated the subject into their daily work. The researchers hypothesized that, for a number of reasons, such workers shied away from addressing this particular area of abuse, despite acknowledging that they were aware that children on their caseload had been abused via the new technologies. Many of those interviewed reported that they were uncertain about how to handle such cases, some questioned whether harmful and abusive online behaviour fell within their purview, while others, on reflection, believed that they or their co-workers should have “noticed something going on.” A cohort of respondents did not recognize online “hazardous behaviour as a problem in itself, and few of them routinely asked questions or attempted to map out their clients’ online behaviour.” Nearly all the informants recognized that they needed to be better informed about online harmful activities, and how children and young people behave in this context.

Developing appropriate recovery services

Appropriate reporting and referral systems must be in place so that children at risk of harm are recognized and referred to the relevant services. In some parts of the world, for example Canada and United Kingdom, child welfare/protection agencies and criminal justice agencies have jointly drawn up procedures for
investigating cases of child sexual abuse with the aim of safeguarding the children concerned and holding the perpetrator responsible. There are assessment and intervention programmes in place to assist children in their recovery and help them understand what has happened to them. However, even in those countries where such connected practice exists, availability of recovery services is limited.

To gain an indicative overview of available rehabilitation and therapeutic services for children, an ad hoc survey of professionals and researchers from 20 countries with expertise in the field of online/offline exploitation and abuse of children was conducted for the purpose of this paper.433 Ten countries – Australia, Bahrain, Denmark, Germany, Iceland, India, Latvia, the Russian Federation, South Africa and the United Kingdom responded – produced the following findings:

- In some countries, there is separate and distinct guidance for police and social workers; in others there is only guidance for police. Some countries have guidance, but it is not adhered to and is out-of-date.

- Staff centres that offer recovery services to children who experience trauma report that they do not feel confident in working with online-related child abuse.

- Funding for services varies across the countries. Some reported that there is no funding at all for such services, while others stated that funding was totally from the government. The remaining countries reported that funding is from a variety of sources, including the government, NGOs, charitable trusts, the ICT industry (Internet service providers and mobile network operators) and private donors.

- Although respondents from six countries replied in the negative when asked if they knew of any research publications regarding recovery needs of children from online abuse within their country, the other four were able to report that some papers had already been written and there are more in the pipeline. Some of the current papers can only be obtained in the native language of the country, limiting opportunity for wider dissemination.

- Six countries were able to describe examples of national/regional police and social workers working together. Some examples were specific investigations that had been carried out and others were of ongoing service delivery, such as hotlines.

- Nine of the 10 countries consulted do not have national systems in place 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. Because of its small size and other demographic factors, 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 who have been victimized throughout the country and runs a multidisciplinary model with police, social workers, lawyers and counsellors who work in partnership. It is able to provide relatively accurate information on the incidence rates of online child victimization in Iceland, but it appears that no further data about the demographic factors regarding the victims is available.

- Four of the country respondents stated that there were no examples of their country working collaboratively on international investigations; one did not know of any, while the remaining five described complex international operations, taking place over months, involving numbers of countries that resulted in children being safeguarded and their perpetrators 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. This review provides a comprehensive analysis of Internet safety issues among adults and children and makes recommendations to ensure the safety of young people and adults navigating the information highway.

These findings clearly reveal a mixed pattern of provision. Although pockets of good practice exist, 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. Indeed, the current paucity of therapeutic services and poor referral networks have led to a concern among some child protection agencies as to whether the process – from recognition to reporting and subsequent interventions by child protection agencies – actually improves the lives of children.434
Chapter 8: Building a protective environment: implications for policy responses

The research findings available suggest that a comprehensive, multi-stakeholder approach to protection should address four interlinked objectives:

1. Empowering children and enhancing resilience to harm – It is imperative that children and young people are empowered both to make informed choices about their online behaviour and, if they do encounter risks, know how to respond and where to go for help. Achieving this goal requires not just working with children and young people but investment in parents and professionals who work with children to ensure that they are able to provide the best possible support for children, and are aware of the range of tools that are available to assist them.

2. Removing impunity for abusers – National governments must take responsibility for introducing the necessary legislation, backed by law enforcement, to send a clear message to those seeking to harm children that these behaviours are unacceptable and will be prosecuted.

3. Reducing availability and access to harm – In coordination with government, the private sector – including the information and communication technology industry, credit card companies and Internet cafe owners – must act to ensure that adequate measures are in place to protect children from inappropriate material, either by its removal, through simple-to-use security settings, or through measures that enable parents to limit access to harmful sites.

4. Promoting recovery and rehabilitation for children exposed to harm – When children are harmed through Internet offences, they should be provided the necessary support and counselling to promote their recovery and rehabilitation.

Governments should adopt overarching strategies for child Internet safety that focus on these four objectives, which should also inform collaboration at the international and regional levels. Developing a comprehensive strategy requires multi-sectoral involvement and coordination. An example of this in practice is the UK Council for Child Internet Safety, created in 2008 to develop and oversee
the implementation of a child Internet safety strategy that brings together government departments and stakeholders including law enforcement, industry, and the civic and public sectors.435

**Objective One: Empower children and enhance resilience to harm**

There are three distinct profiles of children who are potentially at risk of exploitation and abuse in the online environment. The first and largest category is composed of young children used to produce sexual abuse images and videos by parents, caregivers or others with easy access to them. These children have not done anything of their own volition that may have contributed to their being at risk, which is the result of actions by people who are known to them. Child protection strategies should therefore be broadly in line with those for any other group of children being harmed by their parents or other caregivers.

The second profile includes children and young people who are engaged in activities and behaviours on the Internet that could potentially place them at risk. The fact of their agency needs to be built into the protection response. The third profile is children for whom it is others’ behaviour in the ICT environment (bullying and harassment) that exposes them to harm. Effective strategies for empowering and enhancing the resilience of the second and third groups should include: (1) providing the best possible information about the nature of risks associated with their online activities and how to take necessary action to prevent being exposed to harm; (2) the support of key adults in their lives; and (3) helping children and young people know where to go for help when they need it. Children themselves will be a key source of much of that help, drawing on their common culture of Internet usage and their own direct experiences.

Preventive and protective responses to Internet-initiated abuse need to take into account the extent to which children’s online participation, while potentially incorporating risk-taking behaviour, has an important role in their identity construction, self-efficacy and social networking, which should be valued and respected. Responses need to be developed in conjunction with children and young people themselves. Their active participation will contribute to their understanding and confidence, and it will help ensure more effective strategies for empowering children to protect themselves. The nature of the Internet means that there will always be risks. Children and their parents need to understand how to manage those risks as effectively as possible.

**Providing information for children**

Investment in developing appropriate messages on Internet safety and identifying how to reach out to all children is a priority. Information and guidance should be based on accurate analyses of actual risks, taking into account children’s perspectives and experiences, and drawing where possible on the most recent research. Collaboration with children and young people in information and dissemination design will allow for clear, effective messages. Young people better understand children’s realities and experiences and can help craft messages that will be taken seriously. In general, children need to know:

- Their rights online to information, privacy, protection and participation;
- How to safely use the Internet in a responsive and responsible way by respecting the rights and privacy of others;
- The nature of online risks and how to avoid them;
- Where to go when they are concerned or frightened.

Information must be produced and presented in ways that reach children in all situations and speak to their differing ages and capacities. It should also consider young people within a country who do not speak the majority language and those engaged in electronic communication at home, in Internet cafes and via mobile phones.

A variety of outlets for information is needed. Introducing ‘e-safety’ to school curricula, for example, is an effective way of reaching large numbers of children. There will, however, be children and young people out of school who are nevertheless accessing the Internet and alternative ways to reach them need to be developed. These might be delivered through the non-formal school sector, NGOs working with children, public advertising and radio messages.
The development of the Insafe network of national awareness centres across the European Union is an example of an initiative that strengthens information and awareness. At the end of 2010, 30 countries had Insafe centres responsible for providing information, advice and support, running awareness campaigns and monitoring risks.\(^{436}\)

Many countries have developed innovative materials to communicate with children that can be adapted to different country contexts. In 2009, SaferNet Brasil – in partnership with the federal attorney general, federal police, the Special Secretariat for Human Rights at the Office of the President of the Republic and the Brazilian Internet Steering Committee – developed an educational kit on Internet safety. The kit contains booklets, lesson plans, video animation, educational videos, comics, glossaries and tutorials to help educators improve their students’ online safety and to provide educational material to ensure long-term inclusion within Brazilian schools.\(^{437}\) Brazil has also launched the Nética social network to strengthen education and prevention of harm online. The network is open to all teachers and social workers who have been trained in online safety by SaferNet and its partners, and has become a virtual meeting place for discussions and exchanges of material and events on cyberspace safety.\(^{438}\)

The ‘thinkuknow’ website developed by CEOP provides children and young people with accessible information on how to stay protected online. It features up-to-date news on sites children may wish to visit and the latest mobile devices and technology – and explores what is safe, what is not and where children can go for help if they need it. The website offers a child-friendly forum, including cartoons, questions and answers, fact sheets, films and games. It also provides detailed resources about online safety for parents and other caregivers. Perhaps most important, ‘thinkuknow’ has a place for online visitors to report if they feel uncomfortable or worried about someone they are chatting with online. It also runs a major training programme for young people in secondary schools throughout the United Kingdom.\(^{439}\)

In Slovakia, an awareness-raising resource in the form of animated stories has been produced by the Slovak Safer Internet Centre. Using such characters as sheep, a shepherd and his helper, a hunter and a wolf, the cartoons combine traditional Slovak culture with messages on such topics as grooming, paedophilia, racism, and misuse of personal information and photographs. These informative stories have been produced with English subtitles and in sign language as well as in Hungarian, Roma and Slovak.\(^{440}\)

In Venezuela, Manos por la Niñez y Adolescencia (Hands for Children and Adolescents) promotes Internet safety for children, adolescents, adults and Internet cafe owners. Among the group’s activities is disseminating information to children about the law, risks and advantages of Internet use and how to be safe online. It has organized workshops on safer Internet use, moderated by adolescents, which gather information on children’s and parents’ knowledge about the Internet and give them tools to respond if they become a victim of online crime. Steps for the future recommended by participants include collaborating with a software company to develop a safer web page, creation of physical space for dialogue and sharing experiences, and development of cybercafe logos with messages about safer Internet use for children.\(^{441}\)

Governments must take the lead in developing and disseminating information programmes to ensure that approaches are not piecemeal, inconsistent or fragmented. Furthermore, investment in systematic evaluation of these programmes is needed to assess their effectiveness in raising awareness of risk and reducing risk-taking behaviour.

Peer-to-peer approaches to cybersafety programmes are particularly effective. Given the generation gap in both knowledge and understanding of the issues, children and young people are more likely to accept information from their peers or young people slightly older than themselves. Research has also shown that children see themselves as protectors of other children in cases of abusive contacts online. They turn first to each other when in need of help.\(^{442}\) Young people also demonstrate high levels of concern and awareness of risks for younger peers perceived as more vulnerable than themselves.\(^{443}\) These findings point to a potential role for children as peer educators, mentors and advisers, a role that needs to be acknowledged and supported in preventive strategies. Young people should have a significant role in raising the resilience of online communities to provide greater protection.
Effective reporting mechanisms for children

Beyond general information about keeping safe, there is a need for simple, accessible and well-publicized mechanisms for children and young people to report and obtain additional support. The Committee on the Rights of the Child strongly recommends that all countries should establish accessible and child-friendly reporting systems, with child-friendly helplines for protection. Yet many young people have no idea how to report abuse or distressing experiences, or even which agencies are responsible for tackling such concerns. In the Plan India report of 2010, for example, less than 10 per cent of survey participants knew where to report online sexual abuse and exploitation. In addition, even if they know of such resources, many vulnerable children will not report abuse to anyone.

It is important to raise awareness across the entire online community about where to get help with avoiding danger and with responding to harmful experiences online. When access to such resources is provided, resilient children can report grooming attempts and thereby protect more vulnerable children. CEOP has referred to this as ‘raising community resilience’, encouraging social networking site users to report suspicious behaviours to site moderators in order to protect more vulnerable peers and cultivate a more positive online community. Offenders who groom children often target very large numbers in order to increase their chances of finding a vulnerable child susceptible to their advances. If 100 children are solicited by an offender but only one responds to the approach, there are nevertheless another 99 potential chances for a report to be made to law enforcement.

A range of online support to pre-empt abusive situations is available – including hotlines, ‘report abuse’ functions, and online pop-ups and videos with safety messages. In some social networking sites, an icon sits on the home page. If children are concerned at any time about the behaviour of someone communicating with them, one click on the icon will take them to a page where they can identify the type of concern they have and can be linked to a law enforcement agency. Many major social network sites in the United Kingdom now carry the ‘ClickCEOP’ icon, which enables children to report any concern instantly.

These forms of hotline-enabled websites have been successful in removing child sexual abuse images from the Web, reporting criminal activity to law enforcement agencies for further investigation and alerting Internet service providers to criminal activities hosted on their servers. Further evaluation of the level of usage and effectiveness of online ‘panic buttons’ linking websites to hotlines is highly recommended. (See box 1: International Association of Internet Hotlines, below.)

BOX 1: International Association of Internet Hotlines

The International Association of Internet Hotlines (INHOPE) represents and coordinates a worldwide network of hotlines used to report child abuse images, online sexual images and abuse. As of August 2011, there were 40 INHOPE members worldwide in Asia, Australia, Europe and North America; 35 member countries have hotlines. For those countries that do not have hotlines, reports of abuse are passed to the relevant law enforcement agency.

The operations of INHOPE have been described as having a significant role in setting the standards of operation for all hotlines, demonstrating, for example, that groups of smaller countries can establish a shared service or work with an existing hotline.

The INHOPE network has been effective in encouraging law enforcement agencies to respond to reports of illegal content, child abuse images and online grooming, and information from the public has been crucial in identifying the location of child abuse images on the Internet. Some of these reports have led to substantial police action, occasionally on a global scale. If a reported image is found to be illegal and is housed within a country’s jurisdiction, a notice can be issued to the hosting company, requiring it to remove the image. The police can also initiate an investigation. In most jurisdictions, as long as the hosting company acts swiftly to take down the image, it will not be held liable for having hosted the image.

Strengthening parents’ capacities to protect children

As described in Part One, significant numbers of children do not inform their parents
when they encounter difficult or potentially harmful experiences online. Evidence, however, indicates that close communication between parents and children acts as a strong protective factor. As adults lag further behind young people in the use of information and communication technologies, initiatives to improve their knowledge would serve to enhance parental understanding and awareness and help strengthen lines of communication with children.

Programmes are needed to provide parents with information about:

- Types of activities in which children and young people are engaged;
- Benefits and risks associated with the online environment, based on the relevant research (if available) in their country;
- Strategies children and young people need to keep safe;
- How to support children and young people to make safe choices;
- Mechanisms for filtering and blocking harmful sites, while recognizing limitations of highly restrictive impositions on Internet use;
- Potential sources of help and guidance for parents and children;
- Where to report in the event of problems;
- Importance of dialogue and engagement with their children;
- How to talk to their children about sexuality.

Such information is of particular importance for families in communities or societies where parents are less likely to be online themselves or to have any direct experience of the nature of the Internet and the opportunities it offers and risks it presents.

Examples of initiatives in middle and lower income countries include the South Africa Parents Corner, a website that focuses specifically on safety issues in relation to children and young people’s use of mobile phones. The resources for the site come from a company called BulkSMS.com. The global microchip manufacturer Intel sponsors a web site and associated resources available in 24 languages, including specific resources which address online safety for children. The Intel programme has been particularly active in South-East Asia in Cambodia, Malaysia, and Vietnam, and also in Pakistan and Sri Lanka. In India the Data Security Council draws together a wide range of private sector partners in India to promote greater awareness of a range of online hazards, including hazards to children. Since 2003 a group of Indian law schools and lawyers have promoted information and awareness through an organization called Freedom from Abuse of Children through Technology (FACT).

Building the capacities of professionals to support children

The professionals in contact with children on a regular basis – teachers, youth workers, social workers, community development workers and school psychologists – need to be informed about the ways in which children are using the Internet, sensitive to both the benefits and risks associated with its use, and able to provide consistent, constructive and positive guidance to children. They should understand the different types of harmful, abusive and dangerous behaviours online, be able to recognize warning signs and identify symptoms, and be able to talk to young people about their behaviours online and the nature of their relationships.

Given that children are unlikely to divulge what is happening in their online lives, professionals need to be confident in taking a proactive role in exploring with them whether any observed behavioural changes or signs of emotional disturbance are a consequence of their online activities. Although children may initially deny any problem, the intervention opens a door for children who may seek assistance later. Trained professionals already possess many skills required to communicate with and assist children, but they need to be encouraged to build on existing expertise and knowledge about abusive behaviours towards children and to incorporate the growing body of knowledge concerning online abusive and harmful behaviours. In general, the effective integration of understanding of the issues surrounding online related abuse and exploitation into existing child protection services is likely to be more effective than considering the issues as qualitatively different and requiring some form of a specialist stream.

Professionals involved in parent education also need to be up to date on these same issues.
Pre-service and in-service training needs to include components on Internet safety that will enable these professionals to provide appropriate support and guidance for children and young people in the context of their rights to information, freedom of expression, privacy, and protection from violence and all forms of exploitation and abuse. In Thailand, for instance, a digital literacy initiative was established to ensure that ICT users can safely use computers, the Internet, email, smartphones and other new technologies by understanding information technology security, laws on human rights and general safety tips. A training module was developed and some 300 teachers were trained. Those teachers subsequently delivered safety messages to more than 70,000 children.455

**Tackling cyberbullying in schools**

Preventing cyberbullying is a priority for children and young people. Schools must be in the vanguard of adopting strategies to tackle this problem, but they require help from national programmes for guidance and support. Governments need to support the development of initiatives that promote a commitment to zero tolerance of violence and abuse in schools, including cyberspace. ‘Whole school’ approaches involving all members of the school community – including parents – are likely to be most effective. The components of programmes need to raise awareness of the nature, scale and impact of cyberbullying, principles and values of respect and non-violence, mechanisms for reporting, sanctions that encourage insight and understanding of the problem, and monitoring and evaluation of outcomes. In addition, it is important to actively implement educational measures that promote principles of acceptance, respect and decency among students,456 and children need to have a primary role in all stages of this process. One example of a national programme is highlighted in box 2, which describes interventions against cyberbullying in Croatia.

**Involving young people as resources and advocates for Internet safety**

Experience from ECPAT’s work with young people in Africa highlights the diverse strengths young people can bring to the table. In addition

---

**BOX 2: Cyberbullying – Intervening in Croatia**

The Government of Croatia, supported by UNICEF, has backed a national initiative to take on cyberbullying. The approach involves schools, parents and communities in promoting seven elements:

- Awareness that cyberbullying exists;
- Elements of the safety network defined. During this process, students agree on what behaviours they do and do not consider to be acceptable, they discuss what rules should be established and how violations can be handled with a focus on restitution rather than punishment;
- Safety network established and working. This involves peer support, mailbox mechanisms to share concerns and training on how to cope with bullying when it occurs;
- Cooperation across the local community, engaging parents and the wider community;
- Students ask for help. If all the above steps are taken, children should feel more confident about seeking help;
- The school reacts and follows the protocol;
- School is a safer place. Schools that successfully achieve all seven steps are proclaimed ‘Violence-Free Schools’.

The programme involves hundreds of schools. An independent evaluation found significant changes in the environment at participating schools. Students state that they notice violence more, are less afraid and adults react when violence occurs.457
to their intellectual contributions, they added unique perspectives in planning the initiative and skills in mobilizing support, and were far more in touch than adults with the latest technological developments and activities in the online environment. Furthermore, they had creative ideas for countering perpetrators’ efforts to reach children on the Internet and were well placed to provide peer-to-peer education on Internet safety.468

There are several examples of children and young people becoming proactive in campaigns to raise awareness of online risks. In the Philippines, for instance, ECPAT and UNICEF in 2006 supported 75 young people aged 2 to 24 in developing the ‘make IT safe’ campaign.459 The objectives were:

- Create a safe online environment for children and young people;
- Get the information technology industry and Government to make online and interactive technologies safe for children and young people;
- Raise public awareness about the problem of child abuse images;
- Create a positive environment that enables children and young people to confront the phenomenon of child abuse images.

KEY MESSAGE

Children and young people see themselves as protectors of other children. Children turn first to each other when in need of help. Young people demonstrate high levels of concern and awareness of risks for younger siblings, friends and others perceived as more vulnerable than themselves. This suggests a potential role for children and young people as peer educators, mentors and advisers.

Everything Online (EOL), a local franchise that supported ‘make IT safe’, took concrete measures to prevent sexual abuse and exploitation of children via the Internet, including the adoption of a code of conduct and the posting of online safety reminders in their Internet shops. In 2007, the franchise partnered with ECPAT to open an Internet cafe operated by volunteers and young people.460 This promotes guidelines to protect children from harmful material on the Internet and cautions them about risky contacts online or in cafes. Other EOL cybercafe franchisees joined the campaign, leading to a 2008 conference organized with UNICEF that brought together senior government officials including those from public information and mass media, the Centre for Transnational Crimes, the National Bureau of Investigation, the private sector, including business associations, civil society, and children and young people. They identified a series of safety problems confronted at cybercafes and proposed solutions such as pornography site blockers, posted rules prohibiting the surfing of pornography sites and guidance on how to communicate effectively with troublesome customers. Among the many positive conference outcomes was the development of a code of conduct for Internet cafe operators and owners in the Philippines to improve child protection standards in the Internet industry.461

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 on the responsibilities of governments and Internet service providers to ensure better protection of children online.462 The campaign’s focus was to:

- Lobby for codes of conduct in Internet cafes;
- Share experiences on youth mobilization and partnerships;
- Encourage youth partnership with both private and public sectors.

As a result of these youth-led campaigns, participating cybercafe owners in Kenya agreed to codes of conduct that strengthened child protection online. In Benin, some cybercafe owners displayed notices warning customers that their businesses prohibited pornographic content. The success of these youth-led campaigns was grounded by the fact that young people are Internet cafe users and can relate to the movement’s objectives and that cybercafe owners rely on young people as their customer base.

The International Youth Advisory (IYAC) Congress on Internet Safety and Security, launched by the Child Exploitation and Online Protection (CEOP) Centre in London, in July
2008, provided a platform for young people to express their concerns. In a forum with representatives from government, media, law enforcement, education and industry, young people made sure that adults would hear them and act on their concerns about the online environment for children. During the congress, more than 140 youth delegates created the world’s first international charter related to children’s and young people’s experiences in the online environment: the IYAC Children and Young Persons’ Global Online Charter. The charter was intended to serve as a policy proposal for ‘Child Protection in the Converged Environment’ and to be presented for consideration in the 2009 Omnibus Resolution of the Convention on the Rights of the Child.

The charter was intended to serve as a policy proposal for ‘Child Protection in the Converged Environment’ and to be presented for consideration in the 2009 Omnibus Resolution of the Convention on the Rights of the Child.

It is important to ensure that youth participation is not a one-shot event. Rather, their involvement needs to be institutionalized to enable them to influence and bring about change. Young people can contribute their expertise and experience in respect of:

- The nature of the risks and abuses they face;
- Patterns of online activity;
- Levels and forms of needed protection;
- Potential strategies for introducing greater protection;
- Vulnerabilities of particular groups of children;
- Principles governing confidentiality and privacy.

Several countries in the European Union have developed youth panels to raise awareness and share good practices. By sharing their perspectives on experiences online, and on wider protection issues, the youth panels helped those charged with building a protective environment to test materials on their intended audience prior to release, and to fine-tune and direct their campaigns and resources more effectively.

### Objective Two: Remove impunity for abusers

Removing impunity for abusers is essential for preventing and responding to sexual abuse of children in the merged online/offline environment. When abusers are confident that they can act without either social condemnation or risk of prosecution, the problem continues and escalates. Combating abuse and removing impunity requires consistent legislation across nations backed by collaboration with law enforcement. The sexual abuse and exploitation of children online is a global issue, which must be dealt with by action at the national, regional and global levels. There is a grave risk that child sex abusers will concentrate efforts in countries that offer the least protection and where they can more easily exploit children. As outlined by the International Centre for Missing & Exploited Children in 2010, building a “holistic and uniform” approach across jurisdictions is the most effective way to combat sexual exploitation because it:

- Promotes consistency in criminalization and punishment;
- Builds public awareness of the problem;
- Enhances services available to assist victims;
- Bolsters law enforcement efforts at the national and international levels.

The huge differences among existing legal frameworks across the world’s jurisdictions create daunting challenges. Drafting legislation
to protect children in a merged online/offline environment is complex. Establishing a coherent global approach intensifies that challenge significantly.

The international instruments that establish human rights standards and obligations in respect to preventing sexual exploitation and abuse of children in the online environment must be incorporated into national laws that address the need to criminalize harmful behaviour and ensure effective enforcement – and to respect the rights of victims. A holistic approach is required for building an environment that removes abusers’ impunity to prosecution and challenges the ‘cost-benefit’ that is generally weighted in the abuser’s favour. This approach must also seek to secure the indivisible nature of children’s human rights within the process of global implementation of international standards and collaboration and communication among governments. The fundamental building blocks for establishing the legislation and law enforcement framework that are required to remove impunity from abusers are described below.

Effective national legislation

Every country needs to introduce national legislation to bring into force the agreed upon international standards required to protect children from exploitation and abuse in the online/offline environment. The dimensions that need to be considered in drafting legislation, which should be grounded in an explicit commitment to the best interests of the child, include the following:

Clear definitions

Specific definitions in legislation are important in promoting child protection. In countries where ‘child pornography’ or ‘child abuse images’ are not defined, law enforcement and courts have generally failed to include imagery that would otherwise meet the definition intended by international law. The United States Supreme Court case Ashcroft versus Free Speech Coalition, for example, determined that virtual representations of children engaged in sexually explicit activity would not be considered child pornography. Definitions of child pornography as sexually explicit material depicting a person who ‘appears to be a minor’ or ‘is advertised as conveying the impression that the person is depicted as a minor’ were deemed to violate the First Amendment right to free speech. Conversely, South Africa’s legislation bans such virtual representations of children. There is no universally accepted definition of child pornography or child abuse images, and it is incumbent upon each jurisdiction to ensure specificity and clarity in the language of its legislation. Specifically, action is needed to clarify:

- **Definition of child and age of consent** – In order to provide effective protection, national laws must introduce an appropriate definition of a child. Although a person under age 18 may be able to freely consent to sexual relations, such an individual should not legally be able to consent to any form of sexual exploitation, including the creation of child abuse images. Accordingly – and consistent with the definition of a child in the Convention on the Rights of the Child, article 1 – for the purposes of child abuse images, a child should be defined as anyone under the age of 18 years.

- **Definition of child pornography or child abuse images** – At a minimum, the definition should include ‘the visual representation of a child involved in real or simulated sexual acts or the depiction of a child’s sexual organs for the purposes of sexual gratification’. The Committee on the Rights of the Child, consistent with the provisions of the Council of Europe Convention on Cybercrime, has advised governments that legislation be amended to prohibit ‘cartoon’ representations of children. Moreover, the legislation must explicitly address all forms of child abuse images as well as the ways they can be distributed and possessed.

Criminalizing sexual activities with children

In line with the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Abuse, article 18, legislation needs to criminalize engaging in sexual activities with a child under the age of sexual consent, or where “use is made of coercion, force or threats; or abuse is made of a recognised position of trust, authority or influence over the child, including within the family; or abuse is made of a particularly vulnerable situation of the child, notably because of a mental or physical disability or a situation of dependence.”
Criminalizing sexual exploitation and abuse of children

Legislation needs to elaborate a range of offences in order ensure explicit and rigorous protection of children consistent with their human rights, including:

- Possession of child abuse images, regardless of the intent to distribute;
- Downloading or viewing of child abuse images on the Internet and using the Internet to distribute child abuse images;
- Provision of information on where to find child abuse images, for example, providing website addresses, offering advice or taking actions necessary to facilitate the possession or downloading of illegal content;
- Actions of parents or legal guardians who acquiesce to their child's participation in child abuse images (such actions should be recognized as commissioning multiple crimes including rape, sexual exploitation, sexual assault, sexual abuse and the manufacture of child abuse images);
- Grooming offences that involve actions taken by the abuser to 'prepare' the child for a sexual relationship (for example, the Council of Europe Convention on Protection of Children against Sexual Exploitation and Abuse, in article 23, clearly affirms that countries should criminalize any intentional proposal of an adult to meet a child under the age of consent for sexual purposes – and provides a useful model that can be adopted or adapted by countries in other regions of the world);
- Sexual abuse without contact, e.g., criminalization of activities by child-sex offenders that encourage children and young people to participate in sexual activities online.
- Attempt crimes – It is now possible to obtain evidence of an intention to commit a crime against a child in ways that were rarely available previously, for example, from email exchanges, instant messaging logs and text messages. Where such evidence is linked to acts that are preparatory to committing a crime against a child, law enforcement agencies should have the power to make an arrest or otherwise intervene to prevent the intended substantive crime from taking place and to prevent the would be offender from having any direct contact with the child.470

Introducing effective sanctions: penalties and sentencing

If sexual exploitation and abuse of children via the Internet are to be addressed effectively, and impunity removed, it is necessary to ensure that the penalties for committing such crimes are commensurate with the level of harm experienced by the child. Tough sanctions promote a clear message that abusive behaviours are not acceptable, will not be tolerated and will be punished. The Council of Europe Conventions on Cybercrime (article 13) and on the Protection of Children against Sexual Exploitation and Abuse (article 27) reflect the requirement that sanctions for those found guilty of offences of sexual exploitation must be “effective, proportionate and dissuasive,” taking into account their seriousness.

One aspect of this is defining the level of penalties, and there are useful examples from efforts to combat abuse offline. In the United States, for example, the National Center for Missing & Exploited Children has advocated that all legislation against child prostitution and child-sex tourism should carry strict sentences that will be enforced against violators, thereby promoting a deterrent effect. They maintain that fines and misdemeanor classifications are not enough. Legislation should enable aggravating circumstances to be taken into account in determining the response to offences. In addition, some countries have introduced legislative measures subjecting convicted defendants to forfeiture provisions that allow for the confiscation of property, proceeds or assets that resulted from child pornography activities.471 Such elements could well be applied to sexual abuse and exploitation via the Internet.

Avoiding criminal liability of children

National legislation must clearly state that there should be no criminal liability for children involved in online sexual offences. Children should be acknowledged as victims, regardless of whether they were considered to be ‘compliant’ with their abuse or are currently non-cooperative witnesses. Criminal liability must focus on the adult offender, who is
Child Safety Online

responsible for the exploitation of the child, and on the crimes he or she committed against that child.

Legal provisions must allow for the protection of the child as a witness in any judicial proceedings that may occur, including permitting closed-circuit testimony in certain circumstances and establishing guidelines for the presence of victim advocates in the courtroom. The United Nations ‘Guidelines in Justice Matters involving Child Victims and Witnesses of Crime’ offers internationally acknowledged standards and principles, including the right of the child to be protected from hardship during the justice process. These should be extended to child victims of offences committed in the online/offline environment. In addition, where children under 18 are engaged in sexual abuse or harassment online, and the child’s behaviour was deemed to be illegal, the government response 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.472

Consideration might also be given to the issue of sexting. This increasingly widespread practice of young people flirting online and exchanging sexualized or nude images can in some countries result in the prosecution and severe punishment of young people under pornography laws. This response is usually a result of laws that have not been updated to respond to the evolution of technology, or that have a single-focus aim to protect children from sexual predators and, in so doing, fail to look comprehensively at children’s online behaviours.

One approach to resolving this problem might be to amend legislation addressing child abuse images, and other criminalized online actions, to include a special provision for juveniles. This can also be achieved by introducing police charging and prosecutorial guidelines accompanying such legislation, with mitigating and proportionate measures for young people whose online actions bring them into conflict with the law – for example, those who “sext” – so they are not prosecuted as adults or forced to register as sex offenders.473 Legal responses to online child protection concerns can have negative unintended consequences for children, and within the scope of effective responses, must be carefully designed, appropriate, and accompanied by child rights impact assessments to ensure that all children are protected.

Codified timelines

In the criminal justice system, it can take months, if not years, after a child is exploited or abused before an investigation is complete, an alleged offender is arrested, a hearing takes place and a verdict is rendered. Similarly in the civil courts, if a victim is suing the offender for compensation, the process can take many years to come to fruition. During this time the child ages, the technology becomes obsolete and the offender may continue the abuse.474 This could be addressed by the introduction of timelines within relevant legislation. Such timelines can dictate limits on the number of days from the filing of a complaint until a first appearance before a tribunal, the number of months from the first hearing to a final hearing, and the maximum time between a hearing and the final verdict. Guidelines can also be introduced for appeals.

Addressing jurisdiction and extradition

The merged environment is less and less constrained by borders, and in order to protect children, governments must design legislation that covers the actions of their citizens across the globe. Adopting ‘extra-territorial’ criminal laws is essential. Clear guidance for the legislative requirements to achieve this objective can be found in relevant international instruments. The Optional Protocol on the sale of children, child prostitution and child pornography recommends in article 4 that a State Party may establish jurisdiction over offences of sexual exploitation and abuse committed outside their national borders when the victim is a citizen, and when the alleged offender is a citizen or habitually resides in the State Party’s territory. However, article 5 states that the protocol does require that these offences be deemed as extraditable offences in any current or future extradition treaty existing between State Parties. In article 25, the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse goes further and requires that sexual exploitation offences, when committed by one of its nationals in other territories, must also be criminalized. In addition, it requires legislation to enable a person who has his or her habitual residence in the State’s territory (but is not
Effective child-centred law enforcement

To achieve the greatest possible protection for children, law enforcement interventions must cover a broad range of approaches. Some police forces, for example, have adopted intelligence-led, community-based, zero-tolerance or multi-agency partnerships capable of producing effective crime prevention and child protection outcomes.475

In some countries, in order to arrest an offender in the act of soliciting a child, law enforcement members go under cover, posing as teenagers to draw out sex offenders. In such covert operations, the police are able to exploit the same tool of anonymity used by offenders, a strategy not possible in the offline environment.476 Awareness that police are engaged in these proactive investigations of child abuse offenders can act as a deterrent to potential offenders. Such operations also enable the police to obtain documentary evidence through chat logs, which can be used as evidence in court proceedings and avoid the requirement for children’s testimony. Offenders who attempt to download images are confronted by law enforcement, and informed that they have committed a crime and that details have been passed to the relevant national authorities for further investigation.

A study on covert investigations conducted between 2005 and 2008 by the United Kingdom’s New Scotland Yard Paedophile Unit verified that 273 sexual abusers interacted with undercover police officers and were found to have committed sexual offences against children.477 In the United States, a 2006 survey of law enforcement agencies found that 73 per cent of estimated arrests for crimes involving social networking sites were cases that involved undercover operations.478 The results of a study in 2000 suggest that 25 per cent of all arrests for Internet sex crimes against minors were achieved through covert operations. Prosecutions in these cases led to high rates of guilty pleas and low rates of cases being dismissed or dropped.479

There are limitations, however. Although covert operations are undoubtedly a valuable tool for law enforcement agencies in industrialized societies, they involve considerable time and resources and require special investigative training, particularly on how to locate and identify the victim. It is unlikely this strategy would be adopted by many developing countries in the near future.

In all policing approaches, it is imperative that the rights of the child remain at the centre of the investigative process, otherwise there is a risk that she or he will be ‘re-victimized’. The best interests of the child need to be recognized as a primary principle informing the entire law enforcement strategy. Collaboration between law enforcement agencies and agencies with expertise in childcare, child-centred approaches and understanding children’s therapeutic needs are essential. Social workers, teachers and psychologists can provide valuable guidance on 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.

Embedding the interests of the child as a central dimension of the process rather than keeping it as a separate activity is crucial to ensure the best outcomes for children. A strong structural relationship between agencies, recognizing the investigation as a joint activity, is needed from the outset. This will contribute to:

- **Establishing a principled framework**, for example, ensuring that the investigative tactics adopted do not place the child at continuing or further risk. In surveillance operations, police should not actively participate in the abuse or exploitation of children or the receipt of abusive images in order to entrap potential offenders.

- **Ensuring a multi-agency focus**, bringing in all the relevant expertise needed to provide the best possible protection and support for the child, including psychological and counselling support, health care and social work.

- **Highlighting and safeguarding child welfare** during the investigation and ensuring that relevant legislation – as well as advice and guidance for children and young people – are fully understood. Depending on the nature of the case, this may involve considering how to address past or ongoing abuse, making contact with suspects, strategies for undertaking the first contact with children, medical examinations, interviewing strategies, therapeutic needs of the child and advice regarding placement if a child cannot remain with his or her parents.
Enhancing mutual understanding through close cooperation that enables all agencies to better appreciate the tensions and challenges inherent in reducing online offences while protecting children’s best interests. Enhanced understanding will facilitate negotiated strategies for balancing those tensions.

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 online sexual exploitation and abuse of children, enabling different professionals to work collaboratively on cases. (See box 3 above: Holistic and child-centred investigations.)

Cooperation across law enforcement agencies

By serving as a central global point of contact for police, Interpol enables more effective investigations at the local, national and international levels. It also coordinates large-scale investigations involving multiple member countries and utilizes the ‘Green Notice’, an effective law enforcement tool that alerts the international policing community to those offenders who are likely to repeat the same crimes in other countries.

Other global cooperative efforts include: CIRCAMP; the COSPOL Internet Related Child Abuse Material Project, which is a European law enforcement network with a worldwide scope of preventing and detecting online child sexual abuse material; and the Virtual Global Taskforce, made up of law enforcement agencies that work together to fight child abuse online and protect children from abuse. (See box 4: Operation Elm: An international online child abuse investigation, page 83.)

Law enforcement officials use a number of international tools that help gather evidence in criminal cases and facilitate data exchange between national police forces. These include:

- Moyen Automatisé de Recherche des Images Non Autorisées – the Unlawful Images Automatic Search, also known as MARINA, a user-friendly tool that scans suspects’ computers for files related to child abuse images;

- The Investigator’s Dashboard – a tool funded under the European Commission Safer Internet Plus Programme and used to support law enforcement in investigations that involve large quantities of child sexual abuse video material;

- The International Child Sexual Exploitation Image Database – an INTERPOL database that can be securely accessed by accredited investigators regardless of their geographical location and is used to share data with law enforcement agencies via sophisticated image comparison software;

- United States Department of Justice programmes – track and prosecute child abuse images offenders across all jurisdictions, from local to federal to international, and includes the Child Victim Identification Program, the world’s largest database of child abuse images;

BOX 3: Holistic and child-centred investigations

The Child Exploitation Online Protection (CEOP) Centre, based in the United Kingdom, is dedicated to preventing and responding to sexual abuse and exploitation of children and young people. It is primarily a national law enforcement agency whose work includes intelligence gathering and dissemination, public protection through an offender management team, behavioural analysis, financial investigation, victim identification and covert Internet investigation. Additionally, CEOP has a child protection team responsible for ensuring a child-centred strategy for every investigation, developed by social work teams in close consultation with law enforcement staff.

CEOP acts as a single point of contact for sexual abuse and exploitation reports from the public, the Internet, children’s charities and law enforcement through its online reporting mechanism. By bringing together a broad range of expertise, the Centre is able to provide a more holistic approach to preventing sexual exploitation and abuse, law enforcement and recovery. Providing a model for adoption in any country, the commitment to child rights and child protection is central to CEOP’s investigations, and children are never coached in order to secure evidence.
CEOP’s International Child Protection Network – an inclusive approach that shares experience and pools knowledge and is active in Cambodia, Romania, Thailand and Viet Nam, building a network of alliances and partnerships to deliver a holistic approach, spanning geographical borders;486

The European Financial Coalition’s standards of investigation – deals with commercial child abuse images, depending on resources and levels of expertise within law enforcement agencies, and has produced a guidance document for investigations into commercial sites sent to

BOX 4: Operation Elm – An international online child abuse investigation

International collaboration among law enforcement agencies can lead to identification, evidence gathering and arrest of child sexual abusers who operate globally. This was the case in 2007, when an international network of child abusers ran into the long arm of the law, stretching across several country borders.

‘Operation Elm’ was run jointly by members of the Virtual Global Task Force: the Australian Federal Police, the Child Exploitation and Online Protection Centre (UK), Cleveland Police in the United Kingdom, the Metropolitan Police Service (New Scotland Yard’s Paedophile Unit), the Royal Canadian Mounted Police and the United States Department of Homeland Security. The investigation was one of the largest coordinated deployments of undercover officers in the United Kingdom within a child protection investigation.

New Scotland Yard’s Paedophile Unit received information through an Internet forum, where users posted ‘borderline-legal’ images of children and comments that clearly indicated a sexual interest in children. Law enforcement officers recognized the tactic of posting indicative images instead of more explicit child sex abuse images in an attempt to keep the site ‘below the radar’ of law enforcement and prevent the site from being shut down. After making initial contact through the forum, users would then meet other like-minded individuals and organize the exchange of illegal child abuse images in different online sites. Law enforcement identified the principal offender as a senior administrator of the site living in the United Kingdom.

This online forum attracted offenders from around the world, requiring close cooperation among international law enforcement agencies during the investigation. CEOP (UK) coordinated the international investigation, attaching undercover Internet investigators to the operation to obtain more information and identify those suspects who had access to children and posed a risk of perpetrating contact sexual abuse. The Australian Federal Police, the Royal Canadian Mounted Police and the United States Department of Homeland Security took the lead within their jurisdictions. Law enforcement officers seized the server, and were able to identify individuals who accessed the site through their online footprint. Overall, there were 360 suspects, with 130 residing in the United Kingdom.

Given the multitude of suspects, it was crucial to obtain the necessary information to identify both children experiencing ongoing abuse or at risk of being abused, and the offenders. An internationally agreed child protection strategy was developed to guide all interactions between undercover law enforcement agents and suspects while at the same time ensuring compliance with relevant legislation, guidance and good practice standards. This strategy was designed to ensure that no child would be harmed as a result of the undercover deployment, and to maximize access to information relating to children at risk. Appropriate standards and procedures were implemented on discovery of a child victim. Alongside United Kingdom investigative teams was a child protection social worker who monitored and handled issues as they arose. This ensured that all operational decisions were made in the best interests of the child and, if necessary, appropriate referrals to local services would go smoothly. Some 15 children in the United Kingdom and 40 children from around the globe were safeguarded during this investigation.

every national law enforcement agency in Europe.487

Greater investment is needed, however, in refining and expanding tools that can help identify victims, including the development of an international database of images. This would contribute to more effective identification, reduce replication of work across law enforcement agencies, and prevent or minimize repeated viewing of images. Resources would be needed to accurately record incidents of online victimization to better inform law enforcement strategies and to accurately gauge the level of threat. In particular, an international database would enhance the capacities of middle- and low-income countries that otherwise might not have the resources for effective action.

**Cooperation with the private sector**

Because the media and platforms that have been developed and are administered by the private sector provide the infrastructures that are used by abusers, the private sector has an essential responsibility to support action against those who abuse and exploit children. Effective law enforcement in the merged online/offline environment requires the cooperation of ISPs, the online payments industry and other private sector stakeholders. A number of examples of private sector engagement and cooperation now exist:

- In the USA, the Financial Coalition against Child Pornography set up in 2006 by the National Center for Missing & Exploited Children and involving over 30 major banks and other institutions in the online payments industry. It has produced a range of handbooks and guides specifically aimed at combating the trade in online child abuse images.488 In 2009, ICMEC launched the Asia Pacific – Financial Coalition against Child Pornography (APAC-FCACP) to create awareness around the potential use of formal financial systems for such illegal transactions in the Asia region.489

- The European Financial Coalition (EFC), funded by the European Union, involving 20 members drawn from major international credit card companies, the online payments industry, law firms, software companies and non-governmental organizations, led by CEOP during its initial 18 month pilot phase.490 The EFC developed the Flagging and Co-ordination System (FACS), a database of identified websites that traffic in commercial child abuse images. FACS was also designed to ensure coordination in law enforcement operations against commercial sites by flagging those that were already the subject of ongoing investigation, and identifying those that were not.491

- Microsoft has partnered with law enforcement agencies and ISPs in various countries to develop initiatives designed to stop the exploitation of children over the Internet.492

**Mandatory reporting mechanisms**

While the importance of safe and accessible reporting mechanisms has been established, the feasibility of mandatory reporting of child abuse cases should also be considered. None of the international instruments requires introduction of a system of mandatory reporting. The UN Study on Violence against Children presented varying views on the issue and ultimately decided against such a recommendation. Rather, it concluded that governments should review existing reporting mechanisms – and involve children and young adults who have recent experience with child protection systems in the review process.493 However, there may be a stronger case to be made for mandatory reporting in the context of online exploitation and abuse, where a wider group of both witnesses and potential offenders are involved.494

The Committee on the Rights of the Child has continuously stressed that, at a minimum, reporting any instances of suspicion or risk of violence should be required of all professionals working directly with children.495 This would include such individuals as health care and social services professionals, teachers, school counsellors and law enforcement officers, who in their everyday, professional capacity come into contact with children and are responsible for some aspects of their care. The Committee has also argued strongly that, where State Parties have established an obligation for certain professional groups to report child abuse it should be accompanied by appropriate professional training of such staff.496

Concerns have been expressed by many in the child protection field about the efficacy of mandatory reporting. As noted by the 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, the effectiveness of reporting is dependent on the quality of services available to address reports, and risks of over-reporting may increase the burden on child welfare systems and thus decrease capacities to provide assistance, increase adversarial relationships between families and child protection authorities, and discourage families from seeking voluntary help. However, the report affirmed the view of the Committee on the Rights of the Child and argued that reporting by professionals who work with children is appropriate in all societies and has particular importance in respect to younger children who are especially vulnerable and for whom early intervention can help reduce the risk of repeated abuse and long-term harmful consequences.

Some might additionally argue that mandatory reporting should also apply to individuals who may potentially be exposed to child abuse images as a result of their job responsibilities, for example, photo developers and information technology professionals, who discover child abuse images while processing film, repairing a computer or servicing a company computer in an employee’s office. This class of individuals should not be required to search for the illegal material, but instead only report it to the appropriate authorities if found.

**Training**

Given the complexity of the field and the broad range of skills needed to remove impunity for offenders while ensuring the best interests of children, law enforcement, criminal justice and child welfare systems personnel must be afforded training. Practitioners need to have knowledge and skills in:

- International, regional and national legislation relevant to the sexual exploitation and abuse of children in the online/offline environment;
- Application of policing techniques to the online environment;
- New social media and how they can place children at risk of harm;
- Latest research findings on how offenders groom and abuse children.

Furthermore, in order to improve standards of policing in this field and boost the status of the work, key performance indicators on child protection may need to be introduced against which chief police officers would be assessed.

**Objective Three: Reduce availability and access to harm**

Efforts are needed to introduce strategies that both restrict opportunities for potentially offending adults to access abusive material and limit exposure of children and young people to sites, material and experiences likely to cause them harm. While the primary goal is obviously the elimination of online/offline sexual exploitation and abuse of children, the reality is that many millions of images continue to be available on the Internet and are likely to be there for the foreseeable future. Strategies are needed to reduce the numbers of images being created, stored and circulated, and to limit access for both potential abusers and the children who may encounter harmful sites in the course of their Internet use. The continued presence of child abuse images encourages further exploitation of children, leads to increased numbers of abusers, and results in the children concerned being exposed to repeated and indefinite abuse as a consequence of the unremitting circulation of their images. The best interests of children must be protected through the greatest possible effort to ensure that their images are removed as quickly as possible from further circulation, that access to commercial sites is blocked, and that mechanisms are introduced to limit availability and access.

As active agents, 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.

Both the government and the private sector have critical responsibilities in reducing availability and access to harm. As this report identified in its introduction, the ICT industry has it in its powers to develop and introduce new tools to make the Internet safer for children. It also has the responsibility to respect human rights.

There are several practical measures in which the industry can take a lead, providing
easy-to-use technology, implementation and education.

**Developing effective codes of conduct**

Codes of conduct are a common tool of business social responsibility, and this report has mentioned many in its review of initiatives taken. They offer a mechanism through which corporate social behaviours 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 is a challenging exercise. Companies may consider profits, public relations and human rights as mutually antagonistic. Some ISPs, for example, belong to associations where they sign codes of conduct, are willing to explore solutions for protecting minors while online and curb child abuse images. The Internet Service Providers’ Association in South Africa, for instance, has a code of conduct which requires members to take reasonable steps to ensure that they do not offer paid content subscription services to minors without written permission from a parent or guardian. They must also provide Internet access customers with information about procedures and software applications that can be used to assist in the control and monitoring of minors’ access to Internet content.

A positive example of industry’s self-regulation is the reaction in Japan to a campaign in 2009 by the international NGO Equality Now to ban production and sales of Japanese-made rape simulator video games. Soon after the campaign began, a software company stopped selling the game on its own website and an online bookstore removed it from its shopping list. Additionally, the Ethics Organization of Computer Software called for its more than 200 member companies to ban the production of computer games that deal with sexual violence, such as rape, gang rape, incest or sexual molestation and set guidelines for rating adult-content games.

While an important statement of corporate intent, the experience of the UK suggests that codes of conduct which are not linked to demonstrably independent and effective means of monitoring performance will fail to inspire public confidence. A conflict of interest may arise if multinational companies monitor themselves or are monitored by their subcontractors. Without an independent third party acting as a monitor there may be little real incentive for a business entity to observe the terms of the code.

Codes of conduct are relevant for all parts of the Internet industry, large or small. For example, codes of conduct can be designed to protect children who use Internet cafe services from exploitation, can reduce demand for child abuse images, or make it harder to access or purchase these materials. Internet cafe owners, in most of the developing world, the primary source of Internet access for children and young people, can decide to use many different approaches to codes of conduct. Monitoring content can be done through filtering software or a set of rules that can guide how to monitor content manually. This can be discussed and agreed upon by cybercafe owners with the help of the Information Technology Ministry of the respective country. Many Internet cafes have rules advising patrons on how best to use their services while observing moral and ethical conduct, but these are subjective and vary from one person to another based on individual values. These rules are not backed by the law and carry no explicit punitive measures for anyone found violating them. More needs to be done to draft codes of conduct that can guide Internet cafes in how to protect children online.

**BOX 5: Promoting ethical standards in Brazil**

In Brazil Internet Segura (Safer Internet) was established in 2005 initially through the engagement of companies such as Microsoft, American Express and McAfee, but now with many more private sector members. Telefonica’s portal Educarede is provided as a major source of advice and information aimed particularly at schools. ISPs have been encouraged to sign up to a set of ethical codes established by the Código De Auto-Regulamentação De Operadores De Rede e De Serviços Internet of 2007. Those ISPs that agree to its terms undertake to protect individual’s private information, protect ISP end-users and abide by a set of ISP responsibilities.

**Blocking websites**

Internet service providers can use blocking tools to deny access to all or part of a website containing child abuse images. Blocking is a
means of disrupting viewing and distribution of child abuse images. It is controversial as it raises fears about wider censorship. If used, blocking should remain in place only until the illegal material is removed from the source. At that point, the need to obstruct access no longer exists because the illegal material is gone. In addition to Internet service providers, the world’s large search engines also deploy blocking tools to specifically deny access to known web addresses containing child pornographic images. The European NGO Alliance for Child Safety Online recommends the establishment of a single European list, and if possible a single global one, of sites containing child abuse images that should be blocked.507

There is, however, debate about the utility of blocking. For various reasons, blocking tools are not effective by themselves. First, as noted by the European Financial Coalition in 2010, there has been a significant decrease in the number of active commercial sites, the images they contain are generally recycled ad infinitum, and organizers of commercial child sexual abuse websites are distributing images but not producing them.508 In practice, the producers of abuse images are likely to use small, secure areas of the Internet, which are password-protected to share images for free. In other words, websites are not the primary route through which potential abusers access images. Second, removal at the source can be difficult in practice and may be impossible in cases where illegal content is hosted in different countries, and possibly being moved around and among countries on a daily basis. Third, websites exist in which a user can simply input the ‘blocked’ page and will receive immediate access. Alternatively, they can search for one of the many instructional videos online that easily explain how to bypass the service provider’s equipment and any blocking that it has installed.

Outright prohibitions and mandatory filtering at the Internet service provider’s level is generally considered untenable in that protecting children from harmful or inappropriate content would result in an Internet entirely geared towards child safety. The resulting censorship of adult freedoms to access materials on the basis that they were deemed inappropriate for children could inadvertently result in excessive limitations on basic freedoms. Nevertheless, the role of appropriately calibrated blocking measures in targeting child abuse materials remains an important issue for consideration.

**Taking down illegal material**

A great deal of the newer material now available online has been generated by users themselves. In response to the fact that some of this material contains harmful or inappropriate content, most sites that host user-generated content have adopted policies on ‘acceptable use’, which they moderate by taking down material and warning or banning users who misuse the site. The removal of undesirable content from the Internet is described as a ‘notice and take-down regime’.509 When a child abuse image site is identified and reported, the service provider that hosts the site is notified and must take the illegal material down.

Given the volume of material involved – on the video-sharing site YouTube, for example, 48 hours of footage are uploaded every minute510 – moderating abusive activity is a remarkable challenge, and the effectiveness of removal procedures varies widely. The moderation processes of many sites rely entirely on users reporting abuse to the moderators. This can lead to unmanageable volumes of reports, which may result in the abuse being dealt with slowly or not at all. Other approaches include professional moderators, software that automatically identifies content that may be inappropriate or systems whereby reports from users ‘rated’ highly by their peers can be flagged for attention with a higher priority. The latter approach empowers children, young people and adults to be active participants in keeping themselves and others safe online, and making their web communities the kind of place they want to be.511

The ‘notice and take-down’ approach has proved effective in some countries, and is generally fairly feasible across the European Union.512 In the United Kingdom, for example, the 1996 establishment of the Internet Watch Foundation (IWF), with its mandate to identify, report and have child abuse material removed, has led to few abuse sites being hosted there. The IWF operates a hotline for reports of child sexual abuse images from the public, which are then checked and referred to the police if illegal material is found. If the sites are in the United Kingdom, the police will act upon them directly. If they are hosted elsewhere in the world, a report will be submitted to the authorities in the host country. The IWF states that sites are generally removed within weeks, and sites that are traced to hosting in the United Kingdom are removed “within hours.” During 2007, internationally, 71 per cent of websites hosting
sexually abusive images of children were operating for less than 50 days during the year, indicating two ongoing trends: websites were frequently changing servers to avoid detection and removal, and “the effectiveness of efforts to make operations difficult, transient, costly and risky for offenders.”

Research into takedown regimes, however, shows that despite the fact that child abuse images are illegal across many jurisdictions, which might be thought to facilitate effective takedown, their removal is dealt with less speedily than other kinds of illegal Internet activity. Other findings also point to the limited effectiveness of legal frameworks on takedown speeds. Another limitation is that the authorities in individual countries have no say over whether images hosted on servers in another country are taken down or not. Without effective global or regional legislation, takedown can lead to sites being transferred to other jurisdictions rather than actual removal of child abuse material. Part of the challenge lies with inadequate police resources and the priority often given to pursuit of offenders rather than preventive measures, such as removal of sites. Despite limitations, takedown and removal of child abuse material are preferable to blocking as it better protects both children’s safety and adults’ right to Internet access.

Filters and parental control software

There is a wide range of parental control software available to manage children’s access. Parents can set different controls for each family member by assigning individual personal usernames and passwords for logging on. Parental control software is extensively available, often as a free download, as part of another programme, such as an Internet security programme, or integrated into a computer’s operating system. In the United Kingdom, for example, the major consumer Internet service providers – covering 90 per cent of the country’s Internet subscriptions in 2008 – offered filtering products as part of Internet access packages, and most broadband subscriptions came with free filtering programmes. However, evidence shows that despite this availability, just over half of parents actually activate the filtering software on their computers. Some think it is activated automatically, while others feel that their children could bypass the controls anyway. (See box 6 below: Parental control, child protection – A lesson from Hong Kong.)

Safe searching

Most search engines include a ‘safe search’ option that excludes results containing inappropriate images or keywords, but they are not foolproof and cannot ensure that children

BOX 6: Parental control, child protection – A lesson from Hong Kong

The Hong Kong Council of Social Service is raising awareness of effective ways to use online filtering services and software. The ‘Internet Filtering for Junior Internet Users’ campaign will protect young Internet users by: (1) helping parents and the community maintain a list of inappropriate and unsafe websites; (2) providing free filtering services from Internet service providers; (3) educating parents on how to subscribe to and use filtering services.

A parents’ group will maintain and update the website blacklist and specially trained members will review reported websites’ content and assign ‘decency’ levels to each site. The information on the websites – hosted either locally or overseas – will be passed along to the local service providers and, in turn, these companies will provide households with free filtering services that will be added to children’s and young people’s accounts. The filtering service will block the sites blacklisted by the parents’ group. The primary Internet account holder, usually a parent, is responsible for determining the level of ‘decency’ suitable for their children.
will be entirely sheltered from such material. Limitations include:

- The default mode of many search engines is set at a low threshold of safety, requiring the user to actively switch to a higher level of safe search.
- Not all users are aware that this function exists or how to activate it.
- Even when a parent is able to set the ‘safe search’ option, many children have the technological sophistication to turn off the setting to access inappropriate material.
- The capacity to utilize such settings only extends to computers in a fixed location, not mobile phones, which children are increasingly using as the route to the Internet.
- Many children access the Internet from cybercafes, where many users will not want the computers set to high levels of safety.
- Many parents do not use the Internet and have no idea of the type of information to which their children may be exposed.

There is no simple solution to these challenges and, while industry has responsibilities to enable safe searching, technical solutions alone will be insufficient. Parents must be empowered to minimize actual harm and to support their children in making safe choices and behaving wisely online. Additionally, search providers need to offer more accessible, straightforward instructions on how to use safe searches, backed up by information and guidance to parents on the importance of these tools and how to activate them.

While fail-safe search engine protection may seem unattainable, there are ways to improve effectiveness. They include:

- **Parents engaging in more open dialogue** about online activity with their children. Many adults lack understanding and confidence to do this because their children are often more technologically advanced than they are. Gaps can be bridged, however, if parents demonstrate interest, engage in honest discussion about the risks, and show a willingness to respect children’s exploration of the Internet, which may lead children to encounter inappropriate material. The aim should not be merely to restrict access, but to support children to take responsibility in ways that keep them safe.

**Action by the online payments industry**

Historically, credit cards played a major part in developing the trade in online child abuse images. A substantial part of the total online trade in child abuse images was commercially driven. For this reason, the online payments industry has long accepted that it has a particular responsibility to engage closely with law enforcement to combat this illicit traffic. Although there continues to be an important element of commerce involved in the exchange of child abuse images, at a recent high level meeting between EU-US officials it was common ground among the police forces represented that financial gain was no longer the driving force in relation to the larger part of the exchange of child abuse images. This trade is now principally mediated through highly organized, technically literate groups of child sex abusers who exploit Peer2Peer networks.

Through the financial coalitions mentioned earlier and in other ways, major credit card companies and banks in the United States, Europe and the Far East have been collaborating with law enforcement to close down their systems to this type of crime. There is no doubt that the efforts of the financial services industry have helped to drive child sex abuse images off websites and have made it difficult for large scale commerce in these images to be sustained in the way it was in the past. However, means of making anonymous or difficult-to-trace payments online are still available. Pre-paid credit cards and other forms of stored value cards provide a way to transact business online anonymously with little or no risk of being traced. Any anonymous method of skirting the law adds to the difficulty of protecting children and young people from online abuse.
BOX 7: Visa and Action against Exploitation in South East Europe

Since 2009, Visa has funded a project in South East Europe to raise awareness of child exploitation – sharing knowledge about offender behaviour, best practice in protecting children and locating offenders, and improving intelligence flows across borders. This project aims to boost the region’s capacity to combat this crime. It provides training for professionals from government, law enforcement, the judiciary and local NGOs. To date over 300 child protection professionals have been trained across Bulgaria, Poland and Romania. The project has also led to the creation of educational resources in Bulgaria and Romania and the development of new legislation in Poland relating to the distribution of indecent images of children.

Objective Four: Promote recovery and rehabilitation for children exposed to harm

Systems need to be in place to address the reality that – regardless of legislative, policy and protective mechanisms introduced to prevent sexual abuse and exploitation – some children already have experienced harm in the evolving world of cyberspace and its interface with the offline environment and others will continue to experience such harm. 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, and what exists has almost exclusively been undertaken in the industrialized world. Nonetheless, there is sufficient experience of the implications of online abuse and its links with children’s offline experiences to begin to identify key strategies for providing necessary psychosocial support and therapeutic help for children once their abuse has been discovered or disclosed. Such strategies need to be developed within the wider context of child protection work and cannot be addressed independently. They need to be incorporated at an early stage into criminal investigations. Critically, it is necessary to ensure that professionals involved in child protection are sensitized to and understand the particular risks, vulnerabilities and implications of child abuse and exploitation in the online environment and that they acquire the capacities to respond appropriately.

Establishing child-sensitive approaches to discovery during criminal investigations

Children who have been groomed, leading to the production and subsequent distribution of abusive images online – as well as children who have been coerced into such activities by parents or other trusted adults – will usually have great difficulty disclosing what has happened to them. When child abuse images are ‘discovered’, the investigating police officers and child protection social workers have access to exactly what has happened to the child: the images provide proof of the abuse. Unlike other forms of sexual abuse, there is no requirement to build the evidence base regarding whether a crime has been committed. The difficulties faced by children are significantly greater when they are brought into treatment after pictures of abuse have already been exposed by others.

Law enforcement and child welfare agencies need to acknowledge the implications of these differences in the approaches they develop for interviewing. The process must not become yet another experience of abuse for the child. Important issues to consider include:

- Children should not be expected to repeat the details of the abuse they have been subjected to when the images already provide that evidence. Instead, the focus needs to be on such areas as identifying the perpetrator, if not already known, whether other children were involved and where the abuse took place.
- Timing and pace of the interview affect children. When child victims are first informed that images of their abuse have been discovered, they may experience panic and fear as well as feelings of shame. They need to feel supported and be given time to adjust to having become a ‘known victim’. The pace of the disclosure must be aligned with the needs of the child and not be determined by the demands of the criminal justice system.524
The method of recording interviews needs to be considered. Interviews with abused children are often recorded through audio visual equipment – the same conduit that recorded their abuse. Careful thought needs to be given to how such interviews are recorded, bearing in mind that the process intended to protect them may cause further trauma. Children should always be consulted regarding how they feel about being recorded, and serious consideration must be given to their concerns.

Disclosure is a process. As with offline sexual abuse, disclosure needs to be understood as a process, not a one-time event. Victims of abuse and traumatic events rarely reveal all that happened to them in one interview – many need weeks, months and sometimes years to be able to talk about and recover from what they have experienced. Children who feel ashamed and silenced may fear that those asking the questions condemn them or hold them responsible for their abuse. Recognition of these emotions must be given by those conducting the interviews.

Empower the child. The victim needs to be able to decipher the exploiter’s manoeuvring in order to understand what has happened and why. This can help the child reconstruct the experience and transfer responsibility for what occurred to the offender. By enabling the child to have an active role in the disclosure process, she or he can recover the sense of agency and control that has been denied during the experience of abuse.

Address the perpetuity of the abuse. Efforts need to be made to help the child live with the reality that the abusive images may not be removed from the Internet quickly, or at all. Therapeutic interventions that have been developed to help victims who have regular flashbacks to their abuse or some traumatic event in their lives have been found to have some success with children facing this possibility, although the work is still in its infancy.

Families, friends and professionals vary greatly in how they respond to a disclosure. Some believe the child, are supportive and take protective steps; others are disbelieving, and the child may end up distressed and isolated. Disbelief, lack of support or family pressure may result in a retraction of the allegation. Children and adult survivors who have been able to talk about the sexual abuse they have suffered have said that they want, and wanted, the adults in their lives to be proactively protective of them, and they wanted to be able to tell of their experiences in their own way and to be heard and listened to.

All professionals working with children need to know how children who have been the subject of child abuse images are likely to feel and to

---

**BOX 8: Preventing system-induced trauma**

In response to the need to protect abused children from further trauma during the investigative process, some countries have adopted ‘one-stop’ centres where child protection expertise and law enforcement know-how are meshed. Begun in the United States in the 1980s, Child Advocacy Centres are designed to assuage the inevitable strain on children and families during the investigation of a child abuse crime. Ideally, child abuse investigations take place in a child-friendly, comfortable setting that employs a multidisciplinary team of trained personnel from law enforcement, mental health, victim advocacy and health care. The goal is to prevent causing additional trauma while gathering forensic information.

In Canada, for instance, the Edmonton Zebra Child Protection Centre utilizes trained forensic workers who interview child abuse crime victims while police and child welfare workers observe. This process lessens trauma for the child, because he or she is interviewed by one person and therefore does not have to repeat the details of the experience.

The Sexual Assault Referral Centres in the United Kingdom have a similar model, but generally work with adults. Although young people and children have used the services of Sexual Assault Referral Centres, there is a push in the United Kingdom for special programmes for children because their recovery needs and processes are different to those of adults and adolescents. Investigations related to child sexual abuse in the United Kingdom utilize ‘ABE’ (Achieving Best Evidence) interviews, which are designed to minimize trauma and maximize evidence and are based on the Criminal Prosecution Service guidelines.
take the appropriate action to safeguard them. The child needs to:

- Feel believed;
- Be in a safe place;
- Be protected from contact with the perpetrator;
- Be offered therapy at the earliest time;
- Be supported through the process of being a witness.

**Treatment interventions for abused children**

Globally, it is safe to say that there is a history of poor service provision for children who have been sexually abused prior to the onset of the Internet. The situation for those whose abuse has been perpetrated through the new information technologies is worse. Furthermore, there is relatively little knowledge available to date regarding which treatment interventions work for children who have experienced sexual abuse online. There is, however, a considerable body of evidence relating to sexual abuse more broadly that should be used to inform the design of therapeutic services for these children. Services need to be:

- **Holistic** – focusing on children’s needs across all dimensions of their lives and development;
- **Systemic** – involving family, parents and caregivers in order to improve children’s social environments and attachment relationships;
- **Goal specific** – addressing specific issues relating to the child’s sexually harmful behaviour.

The approaches that need to be incorporated in all services are described in the following paragraphs.

**Early intervention**

The earlier therapeutic intervention takes place for an individual after trauma has been experienced, the better the chance of healing and ameliorating the effects.\(^{531}\) The longer between disclosure and commencement of counselling or therapy, the greater the likelihood the child will develop reinforced inappropriate responses and behaviours.

In reality, sexually abused children who must give testimony in court against their abuser are frequently denied therapy pending the outcome of the criminal trial. The prosecutor fears that therapy may taint their evidence and the case could be lost, and the therapist worries that the unique and confidential nature of their work will be jeopardized and their case notes will be demanded by the court. In the United Kingdom, a five-year pilot scheme offering pre-trial therapy to children who had been sexually abused was evaluated. It found that with the right protocols in place none of the children’s confidential records was demanded by the court nor was any case dropped due to therapeutic interventions.\(^{532}\)

**Informed assessment**

Assessment of a child needs to address the known consequences of sexual abuse on children, with a view towards analysing how the recovery work should be directed. The effects of sexual abuse include grief, guilt, fear, inability to trust, cognitive confusion, lack of mastery and control, repressed anger and hostility, blurred boundaries and role confusion, pseudo maturity, failure to complete developmental tasks, depression and poor social skills.\(^{533}\)

**Helping children make sense of their experience**

The overarching approach when assisting children with their recovery from sexual abuse and exploitation needs to help them make sense of what has happened to them. It is important to help them understand how they feel and think and how that affects their behaviour. In therapeutic terms, this is known as a ‘cognitive behavioural approach’ and is often accompanied by other therapies such as drama and art, which assist the child in expressing emotions and being able to ‘move on’ from their victim status.

This process needs to take account of children’s own perceptions of what has happened to them. One way of addressing self-perception has been put forward by BUP-Elefanten, a child and adolescent psychiatric unit in Sweden that treats sexually and physically abused children. It is investigating therapeutic models for assisting children abused via the Internet.\(^{534}\)
BUP-Elefanten has identified three categories of experience:

- **The fooled** – those who were lured into something unexpected;
- **The risk-takers** – those who take risks to meet emotional needs and secure attention;
- **The self-destructive** – those who, for example, sell sex or knowingly engage in abusive relationships.

The degree of shame and complicity felt by the victims will inevitably rise from ‘those fooled’ to those seen as ‘self-destructive’, the latter group tending to see themselves as having autonomy and control, and therefore not recognizing themselves as victims in need of assistance with recovery.535 The status of this group has parallels with that of children abused through prostitution who, because of the trauma bond they have with their pimp, are unable to accept that they are not in control of their situation. It is essential to maintain a dialogue with this emotionally hard-to-reach group and allow them the space and time to come to terms with their predicament.

When working with any child who has been groomed online for sexual abuse, it is essential to understand that most children abused in this way live a conflicting dynamic: They see themselves acting like adults online yet continue to assume their role as a child or young person offline.536

**Supporting and involving parents**

Parents of victims of grooming and sexual abuse are often perplexed about what has happened to their child and are unable to comprehend that their child has been caught up in this type of activity. It is not unusual for mothers, in particular, to show distress and sometimes anger towards their child for ‘getting themselves into the situation’. Similarly, they commonly blame themselves for not knowing what their child was doing online. Therefore, immediate support for the parents is essential if they are going to be able to support their child, and needs to include explanations regarding grooming behaviours online. Current practice around the world too often leaves parents in limbo and feeling impotent to assist.

**Preparation for court**

Children who are required to give evidence in court should be properly prepared for the witness experience. The United Nations Guidelines on Justice in Matters involving Child Victims and Witnesses of Crime provides detailed guidance on the principles and standards that need to be respected when children are attending court.537 Young people and children need information about their role in the proceedings, what they will be expected to say and do, the court process, how to cope when giving evidence, what support will be available, who will be there, what to do if they do not understand something and how to protect their confidentiality.538 The way in which the information is explained is also important. All information provided for children must be in a format appropriate to their age. Child-friendly information packages should be developed that address questions children are likely to have. But written materials alone may not be sufficient; it is often necessary to talk the issues through with the child directly.

Court staff need to be sensitized to the vulnerabilities and challenges child witnesses face in such cases and to understand the need to proceed at the child’s pace, clearly explain the procedures in language that he or she can understand, and take all possible measures to protect the child’s privacy. Child witnesses should also be offered debriefing after the court experience, which can be traumatic.

**Treatment interventions for children who have abused**

Finally, young people who display sexually abusive behaviours online also need treatment. This should be rooted in the same approaches used for those who commit sexually harmful acts offline. Additional issues have been identified that need consideration and are described in the following paragraphs.

**Information-gathering**

A comprehensive assessment of the child and how to effectively intervene through rehabilitation and counselling requires specific information.539 Essential facts include:

- **How children accessed their contacts and any child abuse images** – what sites were accessed via the Internet, what peer-to-peer and social networking sites have been used and what chat rooms were utilized.
- **The motivation of the child** – determining whether the process was self-generated, the
child was encouraged to become involved in illegal behaviour by peer groups or the child was groomed by adults.

- **Materials accessed by the child** – including whether he or she visited adult pornography sites, how many images were downloaded if sites with child abuse images were accessed, the nature of the images and the time frame involved. Knowing the nature of the images may indicate sexual preferences and would therefore provide insight into the child's sexual orientation.

- **Transcripts of email and online chats** – to gain an understanding of the relationships and dynamics between the children and others they have been communicating with.

It is only by doing such investigation at the outset that informed decisions can be made regarding how best to support and help the child. The ability to obtain this necessary information may, however, be obstructed by scarce police resources. Forensic examination of computers takes time and money, and the need for child protection workers to have this information as quickly as possible may conflict with policing priorities.

**Assessment of the child’s development and motivation**

Serious consideration needs to be given to what influenced the child to commit offences online, for example, the child’s level of developmental understanding, the possibility that she or he has been groomed by someone else, the child’s understanding of how indecent images are produced and the abuse inherent in the production of those images, the strength and significance of online relationships and any other sexual behaviours, and the risk of contact offending.

Recognition needs to be given to the potential complexity of the relationship between victim and perpetrator. Denise Moultrie, in her research with adolescents convicted of possession of child abuse images, concluded: “Young people in this sample have undoubtedly been victimized, in that adults have sent them abuse images and communicated with them about the sexual abuse of younger children. However, to regard these young people solely as victims may result unintentionally in the neglect of the needs we would identify for them in addressing their sexual arousal and attitude towards children involved in the abuse images. Online relationships, and the ongoing influence of such, should not be dismissed.” The victim/perpetrator status of young people who have accessed abusive images online needs careful consideration. What might appear to be a straightforward case of a child accessing illegal material might turn out to be a case of a child who is at risk and has been the victim of an adult abuser online.

The attitudes and behaviours that need to be addressed when a child has been abusive online include:

- **Sexual attitudes towards other children** – They may have distorted attitudes regarding victims’ consent and their pleasure in the abusive experience, which need to be challenged.

- **Empathy** – They need help in understanding the production of images, their role in this, the fact that the child in the image is real and has been abused and that it is likely to have had a damaging impact on the child concerned.

- **Denial** – The fact that the abuse has not involved contact often leads to greater detachment from the victim and a denial by the perpetrator that it constitutes abuse. This view is often backed by parents. Work may be needed to raise awareness that viewing of and masturbating to abusive images is abusive behaviour.

- **Positive peer relationships** – Some young people gain their sense of society and relationships from other abusive Internet users. Young people will need help in replacing that peer group with one rooted in positive and appropriate behaviours.

Ultimately, an assessment will need to balance the benefits of supporting the young person to be integrated within the community against the risk of re-offending.

**Working with parents**

As with all interventions with children who have displayed sexually harmful behaviours, it is essential to work with their parents and caregivers. Although they need information and support, many are ill-informed about their
Children’s behaviour online and are unaware of the activities that may take place and how they evolve. Parents and caregivers need information about the nature of children’s behaviour online, how the new technology works and what abusive images actually are. Many of the young people and their families have had no previous contact with children’s services. Parents often want to deny and minimize the seriousness of the offence, particularly if there is no evidence of contact offending. They need to understand the implications if the child’s behaviour leads to a conviction. Some view their child solely as a victim of the adults with whom they have become involved and cannot accept that their child may have been proactive. This is sensitive and difficult work, but essential, because parents’ involvement in monitoring and supervising their children is vital if the behaviours are to change. Effective interventions with this group of young people should, whenever possible, actively involve their families 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 industrialised countries, the global pace of web access, 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 industrialised 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, 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 soon will 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 under-developed 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 information and communications technology 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 likely 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 true particularly in societies where children’s social activity, especially 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 new strategies for response.

Where access is widespread, ICT has in a very short time span 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 developments are still to come, but we do not know yet what they 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 wrong-doing. Children are at the forefront of this dilemma.

For the moment children and young people are pioneers in what many adults might feel to be uncharted territory. The territory, however, is not completely uncharted. Over the past 20 years there has been increasing recognition of the global existence of child sexual abuse and exploitation in other areas of life. Virtually all societies have struggled through the phase of ‘sexual abuse of children doesn’t happen here’ to the recognition that it does, and increasingly systemic approaches to child protection are being put in place, both in terms of prevention and response. Policymakers need to integrate awareness of online-related abuse and exploitation into this broader child protection agenda. Building Internet access for all children and young people means building safer Internet access. 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.
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 (Convention on the Rights of the Child, article 1).

**child abuse images** – 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 (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 (Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, article 2(c)). In this report, ‘child pornography’ is only used in direct quotes or when it refers to specific legislation, judgements or other documents that use this term. Otherwise, the term ‘child abuse images’ is preferred.

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

**child sexual abuse** – As defined in article 18 (1) 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; or
- 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 1.1.a are not intended to govern consensual sexual activities between minors (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 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 technologies, 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.

bulletin boards – Electronic communication forums that host messages and articles connected to a common subject or theme. Bulletin boards work in a similar way to electronic mail (see ‘email’). Participants choose to join a bulletin board, and messages are posted on a news server for all participants to see. Users participate by reading the messages and responding to them.

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 onto a computer for viewing, storage and future access include text files, photographs, videos and music.

e-groups – A group that is centrally controlled and communicates collectively by email; may offer services on an ‘opt-out’ or ‘opt-in’ basis in which an individual chooses to participate after being asked to join the group.

electronic service provider (ESP) or online service provider (OSP) – Any company, organization or individual that provides a service over the Internet. Usually this term is used to distinguish an ESP or an OSP from an Internet Service Provider (ISP) which, historically, provided only access or connectivity to the Internet.

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.

encryption – A process by which data are converted into a format or code that cannot be read or accessed by a person or a computer without the proper key to decode it.

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 ISP. Customised filters have also been developed for mobile phones and consoles.

games console – A device used to play electronic games, especially video games, such as Sony PlayStation or Nintendo Wii. The player typically interacts with the game through a handheld device; newer consoles allow the user to connect directly to the Internet.

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 video-conferencing 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.

Internet Protocol address (IP address) – A string of digits used to represent a computer on the Internet. It can be compared to a telephone number. IP addresses can either be temporary or fixed. Either way they will be directly traceable to a specific machine which was connected to the Internet at a particular time. For this reason IP addresses are of fundamental importance in almost every online child protection or other type of criminal investigation. IP addresses do not tell necessarily
who was using a computer on the Internet at a given time but they normally tell whose Internet account was being used.

**massively multiplayer online role playing games (MMORPG)** – Online games that can be played by large numbers of players simultaneously. Also sometimes referred to as massively multiplayer online (MMO) or massively multiplayer online games (MMOG), some are free, but others have fees to join and ‘virtual’ goods can be bought using ‘real’ money.

**newsgroups** – Online forum or discussion groups. There are thousands of newsgroups on the Internet, covering a vast variety of topics.

**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.

**online service provider (OSP)** – see definition under ‘electronic service provider’ (ESP), above.

**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.

**Usenet** – An Internet service where thousands of newsgroups are located.

**user-generated content** – Material and media created by users of the Internet, rather than by companies. Wikipedia is an example of a user-generated encyclopedia. Videos on YouTube are normally also user-generated.

**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 popular 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.
NOTES


5 The Voices of Youth website, www.voicesofyouth.org, is a forum hosted by UNICEF to enable youth to engage in the top international issues facing them today and allowing them to share their opinions and listen to the stories of others.

6 Australia, Bahrain, Denmark, Germany, Iceland, India, Latvia, Russian Federation, South Africa and the United Kingdom.


11 Ibid, p. 2.


14 Megan’s Law is an amendment to the Jacob Wetterling Crimes Against Children and Sexually Violent Offender Registration Act of 1994 and has become an informal name for legislation in the United States requiring law enforcement authorities to make information available to the public regarding registered sex offenders. Full text available at: http://www.personal-injury-info.net/megans-law-text.htm.


17 Cassell, Justine, and Meg Cramer, ‘High Tech or High Risk: Moral panics about girls online’, in McPherson, Tara ed., Digital Youth, Innovation,
and the Unexpected, Massachusetts Institute of Technology, Cambridge, MA, 2008, p. 70.

18 Ibid., p. 60.


25 Ibid.


28 See, for example: Furedi, Frank, and Jennie Bristow, Licensed to Hug: How child protection policies are poisoning the relationship between the generations and damaging the voluntary sector, Civitas, London, 2008.


39 Palmer, Tink, and Lisa Stacey, Just One Click: Sexual abuse of children and young people through the Internet and mobile phone technology, Barnardo’s, Ilford, UK, 2004.


62 Correspondence with the Child Exploitation and Online Protection Centre, United Kingdom, November 2010 – January 2011.


71 Baartz, D., ‘Australians, the Internet and Technology-Enabled Child Sex Abuse: A statistical


88 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, available at: www.cetic.br/english/. Data are based on surveys of almost 20,000 interviewees.


109. Ibid., p. 4.

110. Ibid., p. 5.

111. Chetty, Iyavar and Antoinette Basson, ‘Report on Internet Usage and the Exposure of Pornography


118 The data presented on mobile phone subscriptions refer to the number of active subscriber identity module (SIM) cards. Given that many people have taken out more than one SIM card, it does not mean that each subscription indicates a different user.


126 Ibid., p. 7.


131 Ibid., p. 10.


136 Ibid., p. 38.


152 Office of Communications, Social Networking: A quantitative and qualitative research report into


157 Ibid., p. 7.


172 Bryce, Joanne, Internet Years Project, Orange, UK, 2009.


177 Interviews with Child Exploitation and Online Protection (CEOP) Centre, London, conducted between October 2010 and April 2011.


181 Brazil Surveys (2009), Accessible online at: http://www.safernet.org.br/site/prevencao/pesquisas/


185 Ibid., pp. 4, 159.


191 Ibid.


193 Ibid.


214 Information provided by the Child Exploitation and Online Protection (CEOP) Centre, London. Interviews with CEOP were conducted between October 2010 and March 2011.

215 Ibid.

216 See, for example: Shariff, Shaheen, Cyber-Bullying: Issues and solutions for the school, the classroom and the home, Routledge, London, 2008.


Cross, Donna, et al., Australian Covert Bullying Prevalence Study, Child Health Promotion Research Centre, Edith Cowan University, Perth, Australia, pp. 171, 184.


Ibid, p. 28.


Ibid., p. 12.


252 Ibid., pp. 18–19.


256 Ibid.


267 Ibid.

268 Ibid., p.55.

269 Personal communication with Tink Palmer, Marry Collins Foundation, UK, March 2010.


277 Ibid., p. 8.


281 Ibid.


300 Ibid., p. 48.


310 Ibid., 5.


327 Ibid.


330 Davidson, Julia, Elena Martellozzo and Mia 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, p. 28–33.


PART TWO: Online/Offline Protection


344 Committee on the Rights of the Child, ‘General Comment No. 13 (2011): The right of the child to freedom from all forms of violence’, CRC/C/GC/13, United Nations, New York, 18 April 2011, pp. 8–18,


353 Ibid., section II. 5.


356 For the time being the US Government maintains a residual role in the management of the Internet through its continued engagement with the Internet Assigned Number Authority (IANA). ICANN “currently performs the IANA functions, on behalf of the United States Government, through a contract with United States Department of Commerce’s National Telecommunications and Information Administration [NTIA]”, see: http://www.nitia.doc.gov/files/ntia/publications/fr_iana_furthernoi_06142011.pdf.

357 John Carr, personal communication, September 2011.


362 See: http://www.itu.int/ITU-T/newslogs/Standards+Need+To+Protect+Children+Online.aspx

363 See Internet Governance Forums, meetings and documentation at: http://www.intgovforum.org/cms/aboutigf


373 Ibid, p. 672-673.


377 Ibid.


381 Ibid., pp. 50, 52.


386 Government of Japan’s response to UNICEF questionnaire in preparation for the Third World
Congress against Commercial Sexual Exploitation of Children, available at: UNICEF Innocenti Research Centre, Florence, Italy


403 See, for example: Cooper, Sharon, ‘Victimology of Child Sexual Abuse Images’, Presentation in ‘Children and Young Persons with Abusive and Violent Experiences Connected to Cyberspace: Challenges for research, rehabilitation, prevention and protection’, Swedish Children’s Welfare Foundation, Stockholm, 2006, pp. 18–21; 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, Tink, and Lisa Stacey, Just One Click: Sexual abuse of children and young people through the Internet and mobile phone technology, Barnardo’s,

405 Ibid.

406 Ibid.


409 For description of Hash Technology see: http://www.law.cornell.edu/uscode/usc_sec_18_00002258—C000-.html


422 Ibid, p. 32.


424 See for example: Police Commissioners’ Conference Electronic Crime Working


427 See: http://www.virtualglobaltaskforce.com

428 Ibid.


433 Survey conducted by Tink Palmer, in October 2010, for the purposes of this paper.


441 Information provided by UNICEF Venezuela, Caracas, 2010.


450 See: http://www.parentscorner.org.za/home-corner/blog/about-us

451 See: http://www.intel.com/about/corporateresponsibility/education/programs/intelteach_ww/index.htm

452 See: http://www.dsci.in/taxonomypage/1

453 See: http://www.asianlaws.org/fact/index.htm


460 Ibid.

461 Ibid.


491 European Financial Coalition against Commercial Sexual Exploitation of Children, ‘14 Months On:


498 Ibid., p. 13.


502 See: http://equalitynow.org.rste057Wlmp01.blackmesh.com/take_action/japan_action332

503 Few of the codes of good practice developed within the UK 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: http://www.education.gov.uk/ukccis/about/a0076277/the-byron-reviews. This rejection was endorsed by the Bailey Review, available at: http://www.education.gov.uk/inthenews/inthenews/a0077662/bailey-review-of-the-commercialisation-and-sexualisation-of-childhood-final-report-published.

504 See: http://www.Internetsegura.org/institucional/institucional.asp

505 See: http://www.educared.org/educa/


513 Internet Watch Foundation, ‘2007 Annual and Charity Report’, IWF, Oakington, UK, 2008, pp. 6, 8,
available at: http://www.iwf.org.uk/assets/media/ IWF%20Annual%20Report%202007.pdf


517 Ibid, p. 95.


521 See, for example: http://news.bbc.co.uk/2/hi/uk_news/2445065.stm on Operation  Avalanche.

522 See: http://john1912.wordpress.com/2011/07/05/microsoft-attacks-online-child-pornography-3/


525 Ibid.


528 Ibid., p. 32.


534 BUP-Elefanten, Centre for treatment of child sexual and physical abuse: http://www.fio.se/Verksamhet/Narsjukvarden-i-centrala-Ostergotland/BUP-kliniker-i-Linkoping/BUP-Elefanten/In-English/

535 Nyman, Anders, Abused Online, BUP-Elefanten (Child and Adolescent Psychiatric Unit) and the Country Council of Östergötland, n.d., available


<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEOP</td>
<td>Child Exploitation and Online Protection Centre (London)</td>
</tr>
<tr>
<td>CETS</td>
<td>Child Exploitation Tracking System</td>
</tr>
<tr>
<td>CHIS</td>
<td>Children’s Charities’ Coalition on Internet Safety</td>
</tr>
<tr>
<td>CIRCAMP</td>
<td>COSPOL Internet Related Child Abuse Material Project</td>
</tr>
<tr>
<td>COE</td>
<td>Council of Europe</td>
</tr>
<tr>
<td>COSPOL</td>
<td>Comprehensive, Operational, Strategic Planning for the Police (European Police Chiefs Taskforce)</td>
</tr>
<tr>
<td>ECPAT</td>
<td>End Child Prostitution, Child Pornography and the Trafficking of Children for Sexual Purposes (Bangkok)</td>
</tr>
<tr>
<td>EFC</td>
<td>European Financial Coalition (against Commercial Sexual Exploitation of Children Online)</td>
</tr>
<tr>
<td>e-NASCO</td>
<td>European NGO Alliance for Child Safety Online (Copenhagen)</td>
</tr>
<tr>
<td>EOL</td>
<td>Everything Online</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>G8</td>
<td>Group of Eight, a forum for the governments of: Canada, France, Germany, Italy, Japan, Russia, the United Kingdom and the United States.</td>
</tr>
<tr>
<td>ICMEC</td>
<td>International Centre for Missing &amp; Exploited Children (Virginia, United States)</td>
</tr>
<tr>
<td>ICT</td>
<td>information and communication technology</td>
</tr>
<tr>
<td>INHOPE</td>
<td>International Association of Internet Hotlines (Amsterdam, the Netherlands)</td>
</tr>
<tr>
<td>INTERPOL</td>
<td>International Criminal Police Organization</td>
</tr>
<tr>
<td>IRC</td>
<td>Innocenti Research Centre (UNICEF)</td>
</tr>
<tr>
<td>ITU</td>
<td>International Telecommunication Union</td>
</tr>
<tr>
<td>IWF</td>
<td>Internet Watch Foundation</td>
</tr>
<tr>
<td>IYAC</td>
<td>International Youth Advisory Congress</td>
</tr>
<tr>
<td>Lanzarote Convention</td>
<td>Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse</td>
</tr>
<tr>
<td>LGBT</td>
<td>lesbian, gay, bisexual and transgender</td>
</tr>
<tr>
<td>make-IT-safe campaign</td>
<td>ECPAT campaign in the Philippines</td>
</tr>
<tr>
<td>MXit</td>
<td>a social network and instant messaging service with millions of users; it is the largest in South Africa</td>
</tr>
<tr>
<td>NGO</td>
<td>non-governmental organization</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>OECD</td>
<td>Organisation for Economic Co-operation and Development</td>
</tr>
<tr>
<td>OPSC</td>
<td>Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography</td>
</tr>
<tr>
<td>Orkut</td>
<td>a social networking and discussion service operated by Google</td>
</tr>
<tr>
<td>SIM</td>
<td>subscriber identity module</td>
</tr>
<tr>
<td>UKCCIS</td>
<td>UK Council for Child Internet Safety</td>
</tr>
<tr>
<td>VGT</td>
<td>Virtual Global Taskforce</td>
</tr>
</tbody>
</table>