International Telecommunication Union

Child Online Protection

Statistical Framework and Indicators 2010

ITU-D

International Telecommunication Union

CHILD ONLINE PROTECTION

STATISTICAL FRAMEWORK AND INDICATORS

Original language of publication: English

International Telecommunication Union
Place des Nations
CH-1211 Geneva, Switzerland

Foreword

The dramatic change associated with the spread of information and communication technologies offers unprecedented opportunities for economic growth and social development in all countries, including in the developing world. At the same time, it also brings new risks and threats to safety and security – especially for children, who are among the most vulnerable members of our societies. With continued growth of the Internet and the Web itself, action needs to be taken to enable future generations of the world's children to grow up safely using the new technologies.

The outcomes of the Geneva and Tunis phases of the World Summit on the Information Society included strong commitments to the protection of children in cyberspace. The Geneva Declaration of Principles stated "We are also committed to ensuring that the development of ICT applications and operation of services respects the rights of children as well as their protection and well-being." The Tunis Agenda declared "We will strengthen action to protect children from abuse and defend their rights in the context of ICTs. In that context, we emphasize that the best interests of the child are a primary consideration."

The ITU Child Online Protection (COP) initiative is a response to those and similar commitments. It is an international collaborative effort led by ITU within the framework of its Global Cybersecurity Agenda (GCA). The COP initiative was launched in 2008 and endorsed by UN Secretary-General, Heads of State, Ministers and heads of international organizations from around the world. It aims to promote global awareness on the importance of child safety in the online world, develop practical tools to assist governments, industry and educators and share their experiences in working to ensure a safe and secure online experience for children everywhere.

This report considers the measurement aspects of child online protection. For the first time, an attempt has been made to provide an overall statistical framework related to the measurement of child online protection with a particular emphasis on measures that are suitable for international comparison. Most importantly, the report recommends a list of indicators related to measuring COP, along with their definitions and suggestions for data collection. The proposed indicators will enable Member States to assess the status of child online safety in their country, and identify aspects of child online protection that may require further effort. The report has been prepared with the objective to reliably measure the problem and monitor the solutions and therefore provides useful guidance to all countries, especially the developing countries, that are interested in monitoring child online safely issues.

The report, which was prepared as an input to the COP initiative and the ITU Council Working Group on Child Online Protection, draws on the experience of countries that have piloted work on measuring COP. It will be subject to regular review as the experience in the measurement of child online protection grows. I am convinced that it will be a useful document for all Member States interested in tackling effectively the subject of child online protection.

Sami Al Basheer Al Morshid
Director, Telecommunication Development Bureau

Acknowledgements

This report was prepared by Sheridan Roberts, consultant to the Market Information and Statistics Division of ITU's Telecommunication Development Bureau, under the supervision of Susan Teltscher. Useful comments and/or material were provided by Susan Teltscher, Esperanza Magpantay, Vanessa Gray, Cristina Bueti, Souheil Marine and Aeree Baik of ITU; John Carr, Secretary of the Children's Charities' Coalition on Internet Safety; Laurent Bernat of the OECD; Kristina Irion, from the Central European University, Budapest; staff of the International Centre for Missing & Exploited Children (ICMEC); staff of the Ministry of Communications and Information Technology (MCIT), Egypt; and Siddharta De of the Australian Bureau of Statistics.

A recent pilot survey of Internet safety issues conducted by Egypt used an earlier draft of this document and collected many of the indicators recommended in this report. Details of the pilot survey are described in chapters 5 and 6.

The desktop publishing was carried out by Nathalie Rollet, and the cover was designed by Nicolas Stauble.

Table of contents

List of examples

List of tables

Chapter 1. Introduction

Child online protection: why is this subject important?

1. The Internet has changed how much of the world's population works, learns, plays and communicates. While this dramatic change has provided great opportunities, it also brings threats to safety and security – especially for children. Dangers include grooming for sexual purposes and cyberbullying. While online, children may be victims of racism and online fraud, and can be exposed to pornographic and violent images. They may also become addicted to spending time online, with the risks and lost opportunities that this entails. With continued growth of Internet penetration and the Web itself, it is likely that without intervention, the situation will worsen.

2. The UN Convention on the Rights of the Child was approved by the United Nations General Assembly in 1989 and spells out the human rights to which the world's children are entitled. In particular, Article 17 refers to access to information by children and protection from "information and material injurious to his or her well-being" (UN General Assembly, 1989).

World Summit on the Information Society (2003 and 2005)

3. In respect of protection of children in cyberspace, the Geneva and Tunis phases of the World Summit on the Information Society (WSIS) resulted in strong commitments. The Geneva *Declaration of Principles* stated "We are also committed to ensuring that the development of ICT applications and operation of services respects the rights of children as well as their protection and well-being." (ITU, 2005)

4. Paragraph 24 of the *Tunis Commitment* (ITU, 2005) recognized "… the role of ICTs in the protection of children and in enhancing the development of children." The commitment continued "We will strengthen action to protect children from abuse and defend their rights in the context of ICTs. In that context, we emphasize that the best interests of the child are a primary consideration."

5. Paragraph 90 of the *Tunis Agenda for the Information Society* (ITU, 2005) dealt with use of information and communication technology (ICT) to achieve internationally agreed development goals and objectives by, among other things, "Incorporating regulatory, self-regulatory, and other effective policies and frameworks to protect children and young people from abuse and exploitation through ICTs into national plans of action and e-strategies."

World Congress III against Sexual Exploitation of Children and Adolescents (2008)

6. The *Adolescent Declaration* from the World Congress III against Sexual Exploitation of Children and Adolescents, held in Brazil in 2008 sought "… strong cyber safety rules which are well propagated on both the websites and within the communities" and called for "… increased development of children's, teachers', parents' and family manuals which address the threats of the internet in addition to providing supplemental information about Sexual Exploitation of Children." (World Congress III against Sexual Exploitation of Children and Adolescents, 2008).

World Telecommunication and Information Society Day 2009

7. The theme of the 2009 World Telecommunication and Information Society Day (WTISD) was protecting children in cyberspace.[1] The International Telecommunication Union (ITU) called upon policy makers, regulators, operators and industry "… to promote the adoption of policies and strategies that will protect children in cyberspace and promote their safe access to online resources."[2] ITU asked its Member States and Sector Members to:

- Create public awareness;
- Identify policies, best practices, tools and resources for adaptation/use in their countries;
- Support ongoing work aimed at developing guidelines for policy makers and regulators;
- Identify risks and vulnerabilities;
- Build resource repositories for common use; and
- Promote capacity building aimed at strengthening the global response.[2]

8. More than 40 countries and organizations have responded to this Call for Action. Additional information can be found at http://www.itu.int/wtisd/2009/initiatives.html.

Worldwide effort: the Child Online Protection (COP) initiative

History and scope

9. The Child Online Protection initiative (www.itu.int/cop) is a specialized programme within the ITU Global Cybersecurity Agenda. It was presented to the ITU Council in 2008 and endorsed by the UN Secretary-General, Heads of State, Ministers and heads of international organizations from around the world.

10. The COP initiative was launched at the end of 2008 and is an international collaboration promoting the online protection of children worldwide. Among other things, it aims to address legal, technical, organizational and procedural issues relevant to protecting children online. Its members are:[3]

- ITU;
- Children's Charities' Coalition on Internet Safety;
- Child Helpline International;
- Cyber Peace Initiative;
- ECPAT International;
- European Network and Information Security Agency;
- European Broadcasting Union;
- European Commission Safer Internet Programme;
- European NGO Alliance for Child Safety Online;
- eWWG;
- Family Online Safety Institute;

- GSM Association;
- iKeepSafe;
- International Criminal Police Organization (Interpol);
- International Centre for Missing & Exploited Children;
- Optenet;
- Microsoft;
- Telecom Italia;
- Telefónica;
- Save the Children;
- United Nations Children's Fund;
- United Nations Office on Drugs and Crime;
- United Nations Interregional Crime and Justice Research Institute;
- United Nations Institute for Disarmament Research; and
- Vodafone Group.

Guidelines on child online protection

11. An important aspect of the COP initiative is a set of guidelines on child online protection. The guidelines were prepared by ITU and a team of contributing authors from the ICT sector and institutions active in child online safety issues. There are four sets of guidelines: for children; parents, guardians and educators, industry and policy makers. They are described below.

Children

12. The *Guidelines for Children on Child Online Protection* are split by age group. Children aged 5-7 are unlikely to be able to apply the *Guidelines* so it is recommended that adults closely supervise their Internet usage using the *Guidelines for Parents, Guardians and Educators on Child Online Protection*. The guidelines for children aged 8-12 use the themes of chatting online and netiquette (being kind and polite), playing online games, reacting to bullying, protecting personal details and identity, and reacting to offensive or illegal content. Children aged 13 or over are characterized by IT proficiency, curiosity and independence. The themes for this group are harmful and illegal content, grooming, bullying, defending privacy, respecting copyright and purchasing online. The *Guidelines* are summarized in the form of contracts (for parents and children) at Appendix 1 (ITU, 2009a).

Parents, guardians and educators

13. The *Guidelines for Parents, Guardians and Educators on Child Online Protection* (ITU, 2009b) attempt to educate on the risks, which are described in some detail. The role of parents and guardians includes communication, educating the child about Internet safety, checking the suitability of websites, being involved in the child's Internet activity, and being aware of different behaviours of the child when online. It also recommends that parents need to teach themselves about online culture in order to carry out their role. The role of educators includes teaching children, setting rules and providing a safe environment at the place of education.

14. The *Guidelines* are presented as themes with one or more 'key areas for consideration'. For parents, guardians and educators, the themes are:

- Safety and security of your personal computer;
- Rules;
- Parents', guardians' and teachers' education;
- Internet sites features review (includes use of filtering and blocking or monitoring programmes);
- Children's education;
- Internet sites safe usage review; and
- Communication.

15. For educators, there are additional themes as follows:

- Safety and security as part of child protection strategies;
- Rules and policies;
- Be inclusive;
- Technological solutions; and
- Internet safety policy.

Industry

16. The *Guidelines for Industry on Child Online Protection* (ITU, 2009c) present a number of case studies. The *Guidelines* are presented as key areas for consideration for the industry segments, ICT industry as a whole, broadcasters, Internet industry and Internet service providers (ISPs), and mobile operators. The key areas for the whole ICT industry cover coordination, cooperation, interoperability and codes of conduct by segment.

17. For broadcasters, the key areas include common complaint rules, common standards and parental consent procedures.

18. Key areas for the Internet industry and ISPs include restricting access to harmful or illegal content; equipping children and their parents with information and easy-to-use tools; using clear and relevant language regarding their services and terms and conditions; responding to and reporting offending content; and evaluating technologies that identify and verify the age of customers.

19. Key areas for mobile operators include ensuring that content is classified in line with national expectations; providing tools that allow access to content to be controlled by the user or a parent/caregiver; clearly signposting the nature of content and services offered; supporting parents and educating consumers; having a clear position on the misuse of services to store or share child sexual abuse content; and supporting law enforcement.

Policy makers

20. The *Guidelines for Policy Makers on Child Online Protection* (ITU, 2009d) present a set of key areas for consideration in the areas of legislation (framework, law enforcement and reporting); national coordination and regulatory policy; and education and awareness (including technical tools such as filtering programmes). A national checklist associated with the key areas for consideration is provided.

21. For the purposes of developing a statistical framework, the *Guidelines* are a useful source of information about the nature of children's Internet use and associated online risks. They describe and define a number of aspects of the topic, such as *social networking sites* and *child abuse material*. They also list and define the key online risks in the following areas: content, contact, conduct, commerce, excessive use and societal. In addition, they describe the stakeholders (known as 'actors' in the statistical framework presented in the report).

Internet Governance Forum (2009)

22. The 2009 Internet Governance Forum (IGF) was hosted by the Arab Republic of Egypt and held at Sharm El Sheikh, Egypt, in November 2009. An important theme of the meeting was the safety of children and young people on the Internet. The meeting discussed measurement issues during the workshop "Child On-line Safety Indicators: Measuring the Un-measurable". The workshop involved panelists from ITU, OECD, Council of Europe, ECPAT International, UK Children's Charities Coalition on Internet Safety and the Ministry of Communications and Information Technology (MCIT), Egypt. Participants discussed current statistical work in the area of child online protection. The workshop concluded that there is a need for standardized data collection and for indicators to monitor efforts in this area.[4]

Regional efforts[5]

OECD

23. The Organisation for Economic Co-operation and Development (OECD) is currently preparing a report on the protection of children online (OECD, 2010). The main objectives of the work are to: enhance mutual understanding of policy approaches to the protection of children online; provide a comparative analysis of those policies; and explore how international co-operation could enhance protection of children online.

24. The report reviews several classifications of online risks and discusses the complexities of a typology. It presents a classification of online risks for children in three broad categories: children as Internet users; children targeted as consumers; and information privacy and security risks. The report includes an overview of policy measures taken by individual members and some non-member countries. Finally, the report discusses characteristics of sound policy-making in this area.

25. OECD held a joint meeting with the Asia-Pacific Economic Cooperation (APEC)[6] in April 2009 on promoting a safer Internet environment for children.[7] Responses from a survey of policymakers on the subject of safe Internet for children were presented. Responses were

provided by Australia, Canada, Philippines, Thailand, US, Denmark, Egypt, EU, Finland, Germany, Hungary, Italy, Korea (Republic of), Mexico, Netherlands, Slovak Republic, Spain, Sweden, Switzerland and Japan (APEC, 2009).

European Commission

26. The European Commission (EC) has developed a policy framework to protect children online. The EC's *Safer Internet Programme* "aims at empowering and protecting children and young people online by awareness-raising initiatives and by fighting illegal and harmful online content and conduct."[8] The Programme adopts and funds a multi-stakeholder approach, including NGOs active in child welfare online, law enforcement bodies working in the field and researchers who collect information about online technologies and children.

27. Of particular interest for this report, the EC *Safer Internet Plus Programme* funded a large research programme, *EU Kids Online* from 2006-2009 (and its successor *EU Kids Online II* from 2009). The findings of the programme are discussed in subsequent chapters.

APEC

28. The Asia-Pacific Economic Cooperation (APEC) has a Telecommunications and Information Working Group (APECTEL), established in 1990.[9] It has a steering group on Security and Prosperity (SPSG), responsible for promoting security and trust in ICT. The joint meeting with OECD was a project of the SPSG.

NGOs

29. There are a number of non-governmental organizations (NGOs) active in the field of COP. They include networks such as INSAFE (the European network of awareness centres) and INHOPE (the International Association of Internet Hotlines, partly funded by the EC Safer Internet Plus Programme).

Individual countries

30. A number of individual countries are actively promoting a safe Internet environment for children. The efforts of OECD member, and some non-member, countries are described in OECD (2010) and include results from a survey of policy makers presented to a joint APEC-OECD meeting held in 2009 (see APEC, 2009). The ITU's Child Online Protection Initiative National Survey was run in 2009 and was directed to national governments (ITU, 2010a). It collected data on the COP initiatives of many developed and developing countries. The APEC-OECD and ITU surveys are described in Chapter 6. The efforts of individual countries in measuring child online protection are described in subsequent chapters.

ITU's statistical work on ICT and telecommunications

31. The International Telecommunication Union collects a range of data on telecommunication/ICT infrastructure, ICT access in households and ICT use by individuals. The resulting indicators, some of which go back as far as 1960, are published in the World Telecommunication/ICT Indicators Database (ITU, 2009e).

32. The telecommunication/ICT infrastructure data are collected from several sources but mainly through an annual survey of ICT ministries and telecommunication authorities. Additional data are obtained from reports provided by telecommunication regulatory authorities, ministries and operators. In some cases, estimates are derived from ITU background documents or other references.

33. Because these data are collected from providers rather than users, they are widely available for both developed and developing countries. They are defined in ITU's *Telecommunication/ICT Indicators Handbook* (ITU, 2010b).

34. Because the area of telecommunications and ICT is rapidly changing, the indicators are updated regularly. Changes are discussed, and revised indicators adopted, at ITU's World Telecommunication/ICT Indicators meeting (WTIM), which is organized regularly.

35. As a member of the Partnership on Measuring ICT for Development, ITU is responsible for a set of core indicators on *Access to, and use of, ICT by households and individuals*. Data are collected from national statistical offices (NSOs) through an annual survey. A major input to the *Partnership*'s work is ITU's *Manual for Measuring ICT Access and Use by Households and Individuals* (ITU, 2009f). More information on the *Partnership,* and its role in standard setting for ICT statistics, may be found in chapters 2 and 3.

Content and structure of this publication

36. Chapter 2 describes a proposed statistical framework for measuring child online protection. It covers scope, actors (*e.g.* children, parents), definitions, classifications, indicators and data collection models. Some of the detail is shown in Annex 2.

37. Chapter 3 looks at measuring the context in which online threats to children arise. An important element of the context is the Internet and the rapid growth in its content and use.

38. Chapters 4, 5 and 6 consider measurement of aspects of the statistical framework as follows: awareness, concerns and attitudes; risk-prone behaviour of children; incidents and children's responses; and, preventive actions. The chapters include recommendations for indicators and measurement approaches.

39. Chapter 7 looks at the statistical challenges involved in measuring child online protection, while Chapter 8 presents conclusions and summarizes the recommendations presented in the report.

40. Annex 1 presents a table showing all the indicators recommended for measuring child online protection at the international level.

41. Annex 2 provides examples of categories used in child online protection surveys and output.

Endnotes

[1] http://www.itu.int/wtisd/2009/index.html. Her Highness Queen Silvia was the Patron of the WTISD 2009.

[2] http://www.itu.int/wtisd/2009/call-for-action.html.

[3] http://www.itu.int/osg/csd/cybersecurity/gca/cop/together.html.

[4] The workshop report was written by Amal Nasralla and can be found at: http://www.intgovforum.org/cms/index.php/component/chronocontact/?chronoformname=Workshopsreports2009View&curr=1&wr=28.

[5] Note that this list is not exhaustive.

[6] The Asia-Pacific Economic Cooperation is a forum for Pacific Rim countries.

[7] APEC-OECD Joint Symposium on Initiatives among Member Economies Promoting a Safer Internet Environment for Children, http://www.oecd.org/document/17/0,3343,en_2649_34255_43301457_1_1_1_1,00.html.

[8] http://ec.europa.eu/information_society/activities/sip/index_en.htm.

[9] http://www.apectelwg.org/.

Chapter 2. Statistical framework for child online protection

What is a statistical framework?

42. A statistical framework describes a particular field of statistics in terms of its content and scope, actors and units, concepts and definitions, classifications, relationships between elements and links to other statistical frameworks. It may also include indicators, sources, methods and/or model surveys.

43. A statistical framework enables the production of accurate and comparable statistics by setting consistent and feasible standards.

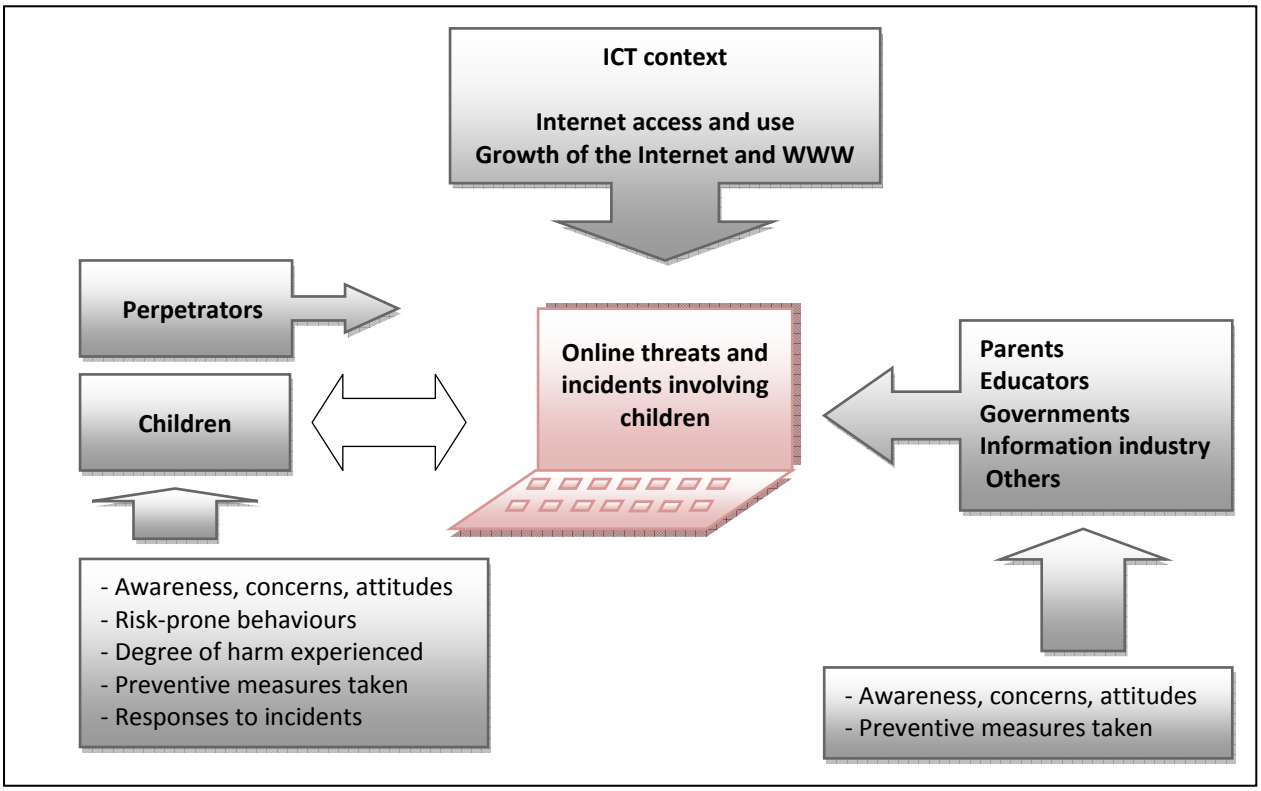
44. This chapter examines existing work and describes a set of statistical standards that covers most of the elements outlined above. Some of the detailed material has been included in Annex 2 for readers wanting more information.

45. The following chapters look more closely at indicators and how they might be collected.

Conceptual overview of child online protection

46. A conceptual overview of child online protection is shown in Figure 1. The overview is highly simplified but shows a broad picture of the measurement coverage for this statistical field. The various elements are further described below.

Figure 1. Child online protection: conceptual overview



Existing statistical frameworks for child online protection

47. While a number of surveys and studies have been carried out on the topic of child online protection, there appears to have been relatively little work done in articulating a statistical framework. The main exception is the EU Kids Online Project funded by the European Commission's (EC) Safer Internet Plus Programme from 2006 to 2009.[1] *EU Kids Online* (Phase 1) was a thematic network designed to co-ordinate research carried out in European countries[2] on how people, especially children and young people, use new media. The research was carried out by the London School of Economics under contract to the EC. It presents a significant body of work in the statistical field with an approach defined by four C's – comparative, contextual, child-centred and critical (Livingstone and Haddon, 2009a). There are a number of outputs from the project including comparative data, policy recommendations, a data repository and best practice and methodology guides.[3]

48. A conceptual view of the topic is articulated in the final *EU Kids Online* report. It is in the form of a matrix showing opportunities and risks for each of three modes of online communication. The matrix is used to analyse available research findings so could also be interpreted as a way of organizing the topic for analytical purposes. Opportunities are split into four areas and risks into another four areas. Modes of communication are Content (child as recipient), Contact (child as participant) and Conduct (child as actor) (Livingstone and Haddon, 2009b). Other elements of the framework are Internet access and use, positive and negative consequences, and contextual elements (market, cultural, educational and political) described in Hasebrink *et al.* (2009).

Scope

49. The proposed scope of this field of statistics is broad and follows the scope covered by the COP guidelines, presented in Chapter 1. The scope is limited to the *Internet*, however it is accessed. Note that many organizations working in, or measuring, this field use a narrower scope, for instance, a focus on the sexual aspects of child safety online. The proposed scope is shown below.

Content – illegal and age inappropriate content on the Internet
Contact – exposure to sexual predators via the Internet
Children's conduct – facilitation by the Internet of risky sexual interactions, posting compromising content, exposure to bullying and opportunity to bully others
Commerce – Internet-enabled acquisition of age-inappropriate goods and services, exposure to scams, identity theft, fraud and similar threats that are economic in nature or are rooted in inadequate data protection or privacy laws.
Excessive use – Internet facilitated excessive use or obsessive behaviour *e.g.* gaming online.
Societal – Internet digital divide, exacerbation of existing disadvantage.
Source: ITU (2009d), Chapter 4.

Actors and units

50. Actors in the proposed statistical framework are generally defined in accordance with the COP guidelines (where they are referred to as "stakeholders"). It is suggested, for some actors, that the concept be broadened to include systems, for instance, educational systems.

51. Units, in a statistical context, can be viewed in several ways. For example, reporting units provide statistical information and statistical units are the units about which information is gathered and tabulated. The relationship between statistical units and actors is explored below.

Children

52. Article 1 of the UN Convention on the Rights of the Child defines a child as "… every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier." That definition is adopted here.

53. In terms of units, the child will also be a statistical unit, though will often not be a reporting unit (a parent or older sibling might have that role). There are often complexities involved in collecting information from and about children. For example, there may be legal or ethical prohibitions on interviewing children below a certain age.[4] The usual alternative to interviewing a child, that is, asking someone else about the activities and experiences of the child, will not always succeed as the respondent may not have the knowledge to respond accurately. The UK study, *UK Children Go Online*, interviewed both parents and children on issues such as preventive measures taken by parents; they found significantly different responses (Livingstone and Bober, 2005).

Parents and guardians

54. Following the COP guidelines, "parent" refers to the natural mother and/or father of a child. A "guardian" is a person to whom guardianship has been granted. As statistical units, parents and guardians do not usually present difficulties. As mentioned above, they will often report in respect of the child/ren for whom they are responsible.

Educators

55. The COP guidelines consider the role of educators to be a broad one, going beyond those who teach in classrooms to include informal educators. It is useful to consider educators in a broader context as well and include the whole education system. The statistical units for educators will vary and include government departments responsible for education, schools and teachers.

Governments

56. Governments have an integral role in many aspects of child online protection. They coordinate stakeholders, undertake education and awareness-raising, legislate and enforce legislation, establish regulatory and self-regulatory regimes, design and implement reporting mechanisms, provide the services required to support victims, and contribute to and adhere to international initiatives and rules. In terms of defining units, government organizations may be

problematic given their range of functions and often hierarchical nature. For a discussion on the challenges presented by measurement of government, see Chapter 8 of OECD (2009a).

Industry

57. "Industry" refers to the elements of the ICT sector that are relevant to discussion of this topic. The COP industry guidelines recognize four industry groups: the ICT industry as a whole, broadcasters, Internet industry and ISPs, and mobile cellular operators. Businesses in these industries are providers of products to the market but can also have a role in how those products are used by children and others. For example, they may undertake awareness-raising, implement technical solutions and engage with Government. In terms of units, these will usually be individual businesses but may also be representatives of businesses, such as industry associations.

Perpetrators

58. Perpetrators are not defined in the COP guidelines and will vary depending on the type of threat they pose. In cases of sexual solicitation, perpetrators will generally be individuals (or networks of like-minded individuals). In cases of consumer fraud, they may be individuals or businesses. Individuals will vary with age, gender, socio-economic status etc. For some online threats, such as bullying and harassment, children themselves are often the main perpetrators.

Other actors

59. Other actors are diverse and include academia, NGOs and international organizations. While their role can be vitally important in preventing online harm to children, in a statistical framework, it is less clear how they should be treated. Some actors will themselves be involved in statistical measurement, others will be involved in direct action and awareness-raising. International organizations, such as ITU, the OECD and the European Commission have several roles in this field. Their activities were discussed in Chapter 1.

Classifying actors

60. Actors are defined above and may be classified in a number of ways. Some classifications may be specific to measurement of child online protection, though most will be general classifications, such as age, gender, industry and geographic classifications, which are presented later in this chapter.

61. An example of a specific COP classification could be one of perpetrators, who could be classified in terms of the nature of their activity (*e.g.* online/offline sexual predator) and/or their relationship to their child victim. The youth questionnaire for the second US Youth Internet Safety Survey (YISS-2)[5] asks a number of questions about the victim's relationship with perpetrators that suggest a *relationship* classification for individual perpetrators as follows:

Someone the victim knew before the incident
Friend or acquaintance from school
Friend or acquaintance from someplace else
Romantic partner (or ex-)
Adult family member
Family member under 18
Someone from work
Neighbour
Other
Someone the victim did not know before the incident
Someone the victim met on the Internet
Someone who had started to feel like a friend
Someone who had started to feel like a close friend
Someone the victim had a romantic online relationship with
Other

62. A perpetrator activity classification will tend to mirror a threats classification though may be more detailed, for example, the YISS-2 youth questionnaire,[6] probes respondents on what the perpetrator did, such as sending sexual pictures of themselves, asking the child to send sexual pictures, calling on the phone, asking to meet with the child, giving gifts etc. Perpetrators' characteristics might also be obtained through crime statistics,[7] for example, Wolak *et al.* (2009) suggest a characteristics classification for US "online predators" as: age, gender, race, substance abuse, history of violence, prior arrests-sex, prior arrests-non sex and whether possessed child pornography.

Statistical standards for context elements of the framework

63. As the conceptual overview in Figure 1 shows, an important part of the statistical field is the prevailing ICT context applying at the national, regional and international level. This report splits the ICT context into two main areas as follows:

- Internet access and use generally, and
- Growth of the Internet and Web.

64. In measurement terms, much of this area has been well articulated, with an established body of concepts, definitions, classifications, indicators and model questions. It is recommended that the field of COP statistics adopts those statistical standards where they are available. It is beyond the scope of this report to suggest standards for ICT context elements where they do not already exist.

65. Available ICT statistics standards are articulated in various publications, including those of the Partnership on Measuring ICT for Development, ITU, the OECD and the UNESCO Institute for Statistics. These can be described briefly as follows:

- The Partnership on Measuring ICT for Development was launched in June 2004, following the first phase of the World Summit on the Information Society (WSIS).[8] The *Partnership* has established a core list of ICT indicators and associated statistical standards to be used by all countries with the aim of providing reliable and internationally comparable ICT statistics. The main reference of relevance to this report is *Core ICT Indicators* (*Partnership,* 2010), which articulates a set of indicators and associated standards across the areas: ICT infrastructure and access; access to, and use of, ICTs by households and individuals; use of ICTs by businesses; the ICT sector; trade in ICT goods; and ICT in education.
- ITU is responsible for standard-setting and data collection for the core indicators on *ICT infrastructure and access* and *Access to, and use of, ICTs by households and individuals*. More information on these activities can be found in Chapter 1. As an input to the *Partnership*, ITU has developed a manual for collection of data on access to, and use of, ICT by households and individuals (see ITU, 2009f).
- The OECD is a leader in establishing standards for measuring the information society. OECD's *Guide to Measuring the Information Society* (2005, 2009a) brings these standards together.
- The UNESCO Institute for Statistics (UIS) is responsible for the core indicators on ICT in education. In late 2009, it released *Guide to Measuring Information and Communication Technologies (ICT) in Education,* which articulates these and other ICT in education indicators (UIS, 2009).

66. Eurostat and its Member States are active in measuring access to, and use of, ICT through the annual community surveys on ICT usage in households and by individuals. This work involves the development of concepts and classifications suitable for questions on household surveys. Eurostat produces a methodological manual for its household and business ICT use surveys (for example, see Eurostat, 2009a).

67. The United Nations Conference on Trade and Development (UNCTAD) is responsible for the economic indicators covering business use of ICT, the ICT sector and trade in ICT goods. These areas are less pertinent to this report, although for completeness, a reference to UNCTAD's work is included (see UNCTAD, 2009).

68. Indicators and data sources for ICT context elements are proposed in Chapter 3.

General classifications

69. Existing general classifications can be applied to elements of the framework. For instance, human actors can be classified by age and gender, incidents can be classified by region or country level of development. There is a large number of such classifications that could be used. A minimal set, likely to be applicable to all countries, is proposed in this report.

70. General classifications recommended for child online protection measurement should be defined in terms of existing statistical frameworks, most of which are articulated by the United Nations. The recommended classifications are as follows:

Age

71. An age classification can be applied to children, parents and perpetrators. It is recommended that age ranges be consistent with the 5-year age ranges adopted by UNSD (2008a) for population censuses. ITU (2009f) proposes the following ranges for measuring use of ICT by individuals: 1 to 4, 5 to 9, 10 to 14, 15 to 24; 25 to 34; 35 to 44; 45 to 54; 55 to 64; 65 to 74, 75 or over. Given that the definition of a child adopted in this report is someone under the age of 18, it will be necessary to depart from the existing guidelines and split the 15-24 age group (into 15-17 and 18-24) if at all possible (or, if not, at least into 15-19 and 20-24 years in accordance with UNSD age ranges). In addition, it may be of value to further split the age range 10-14, reflecting rapid development by children in this age group.

Gender

72. The gender classification is male/female and can be applied to children, parents and perpetrators.

Industry

73. An industry classification can be applied to industry actors. It is recommended that the internationally recognized definitions of the *ICT* and *Content and media* sectors be used for this field of study where an industry classification is needed. The *ICT sector* has been defined by the OECD according to the standard international industrial classification, ISIC. Details may be found in OECD (2009a) and *Partnership* (2010). OECD has also defined a *Content and media sector* based on ISIC, Revision 4 (OECD, 2009a). The ICT sector and the Content and media sector as defined by OECD are recognized as alternative aggregations in ISIC Rev. 4 (UNSD, 2008b).

74. The *ICT industry* detailed in the COP industry guidelines includes elements of the OECD's ICT sector and Content and media sector. The elements in the *Guidelines* are: the ICT industry as a whole, broadcasters, the Internet industry and ISPs, and mobile operators. In terms of ISIC Rev. 4, these elements can be defined and further split as follows:

- Broadcasters are included in the Content and media sector. In ISIC Rev. 4, their activities are in Division 60, Programming and broadcasting activities. This division is split into Radio broadcasting and Television programming and broadcasting activities.
- ISPs and mobile operators are in the ICT sector and are included in ISIC Rev. 4 Division 61, Telecommunications. The division is dissected according to the nature of the technology used (wired/wireless/satellite/other telecommunications activities). Mobile operators are included in class 6120, Wireless telecommunications activities. ISPs may be included in any of the classes of Division 61, depending on the nature and ownership of the technology infrastructure used. ISPs that are not operators of telecommunications infrastructure are included in 6190, Other telecommunications activities.
- The "Internet industry", per the COP guidelines, is a little harder to define in terms of ISIC Rev. 4. A number of activities may be conducted over the Internet or in other ways. In ISIC Rev. 4, these tend to be classified according to the activity (*e.g.* retailing, education) rather than the medium (Internet). In particular, Internet publishing activities are included in ISIC Rev. 4, Division 58, Publishing activities, which is part of the Content and media sector.

Broadcasting activities may also occur over the Internet (*e.g.* Internet radio stations). Within the ICT sector, the activities of providing Internet search facilities and operating websites that act as portals to the Internet are included in Division 63, Information service activities. Provision of Internet advertising is included in Division 73, Advertising and market research. It can be seen that the "Internet industry" can be viewed in terms of provision of infrastructure and content. Both are likely to be relevant to the topic of child online protection.

Other classifications

75. A number of other general classifications are possible. They include classifications that compare countries (region and level of development), socio-economic status (for instance, Livingstone and Haddon, 2009b), urban/rural splits, income (for instance, household income) and whether or not a child belongs to a high-risk category. Because these classifications are of less relevance, or difficult to define or collect, they are not recommended for this statistical framework.[9]

Defining and classifying online safety elements

76. Central to standards for measuring child online protection is the definition and classification of online safety elements of the framework. For the purposes of this report, these are:

- Children's risk-prone behaviour (activities and time spent online);
- Online threats and incidents;
- Children's responses to those incidents; and
- Preventive measures.

77. At the outset, it should be understood that a classification for presenting output or for analysing data will not necessarily be the same as one used for collecting data. In this report, we therefore distinguish *output* and *input* classifications. In addition, a classification used for statistical purposes will generally have some rules that make it suitable for that purpose. These include being comprehensive and having no overlapping categories. Some of the classifications presented below do not comply with those rules.

Children's risk-prone behaviour

78. Some of the online behaviour of children and young people may be considered 'risky' in terms of exposure to online threats. For the purposes of this report, risk-prone behaviour includes certain activities that could increase risk and the amount of time spent online.[10] A number of surveys and studies have examined these activities, which broadly include:

- Propensity to generate content (called user-created/generated content, Web 2.0 and participative web). OECD (2008) discusses user-created content (UCC), which it characterizes as publicly available over the Internet, non-commercial and reflecting creative effort. UCC activities include social networking, virtual worlds, blogs, wikis,

feedback, sharing photos, videos etc. OECD notes the relationship between UCC and the protection of children and expects UCC to grow due to new drivers such as the increased use of mobile phones to access the Internet and mobile content (OECD, 2008);

- Communicating online via email, instant messaging, chat sites and online forums etc. The child may not know some of those with whom they are communicating. This could pose a particular threat (such as 'online grooming'[11]);
- Time spent online (measuring excessive use of the Internet); and
- Other risk-prone behaviours per the recommended scope of COP measurement include online gaming and use of the Internet to acquire goods and services.

79. Various surveys have effectively created classifications of risk-prone behaviours by asking about those behaviours in questionnaires. These are described below and more information can be found in Annex 2.

- A major objective of the National Teen Internet surveys of 2006 and 2007 (US) conducted by Cox Communications (2007) was to measure online teenagers' (13-17 year olds) tendency to exhibit potentially risky behavior via the Internet and other forms of virtual communication (such as, text, email, and instant messaging). Risky behaviours included whether teens had posted a fake age online, created online profiles, created public online profiles, and posted personal information or photos of themselves online.
- The Eurobarometer 2007 Survey (Safer Internet for children) was a qualitative study of 29 European countries, aimed at children aged 9-10 and 12-14. Among other things, the study asked about various activities, some of which could be considered risky (EC, 2007).
- The Crimes against Children Research Center (US) ran studies in 2000 and 2005 (YISS-1 and YISS-2) (Wolak *et al.*, 2006). They conducted telephone interviews with national samples of Internet users aged 10 to 17 and asked about various risky activities.
- Some national statistical offices also collect information on risk-prone Internet activities. They include the European countries (through the Eurostat model survey), Singapore (IDA), Australia (ABS), Thailand (National Statistical Office of Thailand) and the Republic of Korea (NIDA).
- Thailand, in its 2007 and 2008-09 ICT Household Survey, asked about Internet activities of respondents (including children) and included the categories "Chatroom & Webboard" and "Game" (National Statistical Office of Thailand, 2007; 2010).
- The Republic of Korea conducted a survey specifically on SNS (social networking service) usage by individuals in 2009. Services were categorized as: Online club/community, Blog/minihompy, Instant messenger, Personal networking site and Virtual reality service (NIDA, 2009). More information on this survey is presented in Chapter 5.
- EU Kids Online II will also collect information from children aged 9-16 about their Internet activities. Its categories include activities similar to those described above but, in addition, the questionnaire asks children about posting videos online, virtual worlds and whether an avatar had been created. It also probes children on the type of online communication they undertake, asks details of social networking site profiles and risky online activities such as: looking for new friends, giving personal information to those met online, pretending to be different and sending photos or videos of him/herself to online contacts.[12]

80. Several different types of surveys can be used to measure the time that individuals spend online. They include time use surveys, ICT use surveys and surveys dealing specifically with child online protection. For a statistical framework, the classifications and definitions used in such surveys are of interest. Statistical standards for time use surveys are provided by the United Nations Statistics Division (UNSD), which provides a time use activity classification (the *International Classification of Activities for Time-Use Statistics*). It is not particularly useful for measuring COP as it only has one ICT category (using mass media – computer technology). Other ICT-specific surveys may also include questions on time spent online. They include household ICT use surveys and COP surveys. They ask a variety of questions and tend to group responses by age group. More information on these surveys can be found in Chapter 4.

Recommendations

Recommended classification, with definitions, for a minimal set of risk-prone behaviours	**Source**
Purchasing or ordering goods or services *Purchase orders placed via the Internet whether or not payment was made online. Orders that were cancelled or not completed are excluded. Includes purchasing of products such as music, travel and accommodation via the Internet (Partnership, 2010).*	HH9
Playing or downloading video games or computer games *Includes file sharing games and playing games online, either paid or free of charge (Partnership, 2010).*	HH9
Downloading movies, images, music, watching TV or video, or listening to radio or music, split into:	HH9
Downloading movies, videos, images, TV programmes or music *Includes file sharing (Partnership, 2010).*	*Split*
Watching TV or video, or listening to radio or music *Includes using web radio or web television (Partnership, 2010).*	*Split*
Posting information or instant messaging, split into:	HH9
Posting messages to chat sites, social networking sites, blogs, newsgroups and other online discussion forums; use of instant messaging *A chat site (also called a chatroom) can be defined as a virtual room, where participants have a chat session. Social networking sites (e.g. MySpace, Facebook) are mostly used for uploading and sharing of audio and video content, they also allow posting of messages and participation in forums on specific topics of interest. A blog (weblog) is a website where entries are made such as in a journal or diary. A typical blog combines text, images, and links to other blogs, web pages, and other media related to the topic of interest and can allow the posting of messages from others. Newsgroups and other online discussion forums cover a variety of interests. The members of a newsgroup view and post messages via a news server on the Internet. Instant messaging means real-time communication between people on the basis of typed text (adapted from Eurostat Methodological Manual, Eurostat 2009a).*	Eurostat 2010
Uploading self-created content (text, images, photos, videos, music etc.) to any website to be shared[13] *This can involve uploading of own produced content to own website or to any other website with the purpose of sharing it with others (Eurostat Methodological Manual, Eurostat 2009a).*	Eurostat 2010

81. A minimal and reasonably broad classification of risk-prone activities is recommended and shown above. It is based on several of the existing activities in the *Partnership*'s core ICT indicator, HH9, *Internet activities undertaken by individuals in the last 12 months* and Eurostat's 2010 model questionnaire for the Community Survey on ICT usage in Households and by Individuals. Countries wishing to split categories further or add categories can do so.[14] Of particular interest may be the addition of categories on whether the child has one or more online profiles on a social networking site and what kind of information is publicly available (*e.g.*

real name, contact details). Split categories could show details of information posted *e.g.* photographs.

82. Regarding measurement of time spent online, more standardization of the types of questions asked and the age ranges would be very useful. It is suggested that the best vehicle for such questions is a national ICT household survey. Time use surveys are not recommended as they are directed to adults and there are complications in measuring time spent using ICT (necessitating a secondary classification of 'technology used' to carry out a particular activity).

Online threats and incidents

83. Online threats (or risks) and incidents are treated together because they are closely related in a definitional and classification sense.

84. There are a number of classification models that have been articulated for online threats and incidents. Some are not statistical in nature and are often implied rather than articulated as a classification. Some have been developed to present or analyse data (output classifications) and others for use on questionnaires (input classifications). These are also often implied. A selection of classifications is presented below and in Annex 2.

85. The COP Guidelines are not statistical in nature and contain implicit definitions and a classification of threats and incidents. In particular, the *Guidelines for Policy Makers on Child Online Protection* describe key risks as shown below.

Content
The Internet's ability to expose children and young people to illegal content, *e.g.* child abuse material (CAM)
The Internet's ability to expose children and young people to legal but age inappropriate material *e.g.* very violent imagery.
Contact
The Internet's ability to expose children and young people to sexual predators, be they adults or other minors.
The way in which the Internet may expose children to harmful online communities such as sites that encourage anorexia, self-harm or suicide – as well as sources of political influence espousing violence, hate and political extremism.
Conduct
The way in which the Internet facilitates and can promote risky sexual interactions between children themselves, including encouraging them to take and post pictures of themselves or others (sexting) which, aside from being harmful, may also be illegal.
The way in which some aspects of the Internet encourage children to place in the public domain information about themselves, or post pictures or videos or text which might compromise their personal safety or jeopardize a number of career options for them in the future.
The Internet's ability to expose children and young people to bullying and to allow or promote an environment in which children and young people are encouraged to bully others.
Commerce
The ways in which the Internet has enabled children to access or acquire age inappropriate goods and services, typically goods and services that they could not purchase in person from a shop.
The Internet's ability to expose children and young people to scams, identity theft, fraud and similar threats that are economic in nature or are rooted in inadequate data protection or privacy laws.

Excessive use
The way the Internet seems, with some children and young people, to have encouraged forms of obsessive behavior or excessive use which may have deleterious effects on children's and young people's health or social skills, or both. Games and gaming over the Internet often feature in this type of online behavior, which may be referred to as a form of addiction.
Societal
The way the Internet has opened up a new digital divide among children and young people, both in terms of those who have ready and convenient access to it at home, school and elsewhere, and those who do not; between those who are confident and proficient users of it and those who are not. This divide threatens to entrench or widen existing patterns of advantage and disadvantage or perhaps create new divides.
The potential of the Internet to compound and even magnify the existing vulnerabilities of particular children and young people and add to adversities that they may face in the offline world.

86. The EU Kids Online Project has suggested four groups of risks cross-classified by the mode of communication: child as recipient, child as participant and child as actor (Livingstone and Haddon, 2009b). This results in 12 areas of risk, considered to comprise an *output classification*, as follows:

Risks	Child as recipient	Child as participant	Child as actor
Commercial	Advertising, spam, sponsorship	Tracking/harvesting personal information	Gambling, illegal downloads, hacking
Aggressive	Violent/gruesome/hateful content	Being bullied, harassed or stalked	Bullying or harassing another
Sexual	Pornographic/harmful sexual content	Meeting strangers, being groomed	Creating/uploading pornographic material
Values	Racist, biased info/ advice (*e.g.* drugs)	Self-harm, unwelcome persuasion	Providing advice *e.g.* suicide/pro-anorexia

87. OECD (2010) has reviewed several existing classifications and describes the complex nature of such a classification (which it calls a *typology*). OECD suggests other possible criteria for inclusion in a classification of risks, such as whether the child is interacting with a human or a machine and which actors are involved in the risky interaction, for example, between children or between a child and an adult (OECD, 2010). The scope of OECD remit in the topic of child online protection excludes issues related to online child pornography and sexual exploitation (as these are to be addressed in a contribution from the Council of Europe). OECD proposes a typology of online risks for children, with definitions and categories as follows:

Broad category	Second level	Third level
Children as Internet users (Internet as medium of child's exposure to content or child's interaction with others)	Content risks	Illegal and harmful content, harmful advice
	Contact risks	Cybergrooming, online harassment, illegal interaction, problematic content sharing
Children targeted as consumers online	Online marketing	Child inappropriate online marketing, online marketing for illegal or regulated products, unhealthy food and drinks
	Overspending	
	Fraudulent transactions	Online fraud, online scams, identity theft
Information privacy and security risks (risks that all Internet users face but where children are particularly vulnerable)	Information privacy	Personal data, oversharing, unforeseen and long term consequences
	Information security	Malicious code, commercial spyware, online scams, identity theft

88. Various surveys and reports have created or used classifications of online risks and incidents. These are described below and details can be found in Annex 2.

89. INHOPE, the International Association of Internet Hotlines, is a NGO umbrella group. It represents 36 hotlines in 31 countries, covering 21 of the 27 EU member states, as well as Australia, Canada, Iceland, Japan, Russia, South Africa, Korea (Republic of), Taiwan (Province of China) and the United States. Each national hotline deals with what is considered to be illegal content in that country.

90. INHOPE statistics classify and measure processed reports. Their classification of reports (an *output classification*) uses illegality under national law as a defining characteristic of some categories. The classification can be found in Annex 2.

91. One could also devise classifications based on the severity of risk. *EU Kids Online* classifies the overall level of risk as low, medium and high (Livingstone and Haddon, 2009b). Other approaches may rate some threats to children as more serious than others. For instance, paedophile crimes might be considered more serious than risks to children's development arising from time spent playing games online.

92. It is fairly obvious that the task of devising a classification of online risks and incidents suitable for statistical purposes will not be straightforward. While the subject is inherently complex and multi-dimensional, for statistical purposes, simpler or more limited *input classifications* are likely to be required where they are to be included on a questionnaire. In this context, it is useful to look at some classifications that have been used on questionnaires.

93. The Child Online Protection Initiative National Survey was run by ITU in 2009. It was an online survey directed to national governments, using tickbox responses. The first block of questions, ("The problems"), constitutes an input classification at a broad level and is shown in Annex 2.

94. Perhaps the most internationally comparable surveys in this area are those conducted by Eurobarometer and covering the European countries. Eurobarometer 2008 (*Towards a safer use of the Internet for children in the EU – a parents' perspective*) asked parents about situations on the Internet that children could not handle. The classification of *situations* is shown in Annex 2 (EC, 2008).

95. The Eurobarometer 2005 Survey (EC, 2006) asked a yes/no question of parents "Do you think your child has ever encountered harmful or illegal content on the Internet?" A follow-up question asked where the incident occurred.

96. Eurostat's 2010 country questionnaire for the Community Survey on ICT Usage in Households and by Individuals, includes a module on Internet security. The security related problems asked about include "Children accessing inappropriate web-sites or connecting with potentially dangerous persons from a computer within the household" (Eurostat, 2009b).

97. The second US Youth Internet Safety Survey (YISS-2) (Wolak *et al.*, 2006) asked about three kinds of victimization – sexual solicitation and approaches, unwanted exposure to sexual material, and harassment, with follow up questions on what activity the respondents were

doing when the incident occurred. Classifications of incidents and activities can be constructed from the question wording, as shown in Annex 2.[15]

98. In 2009, the Australian Bureau of Statistics (ABS) conducted a Children's Participation in Cultural and Leisure Activities (CPCLA) Survey. As in previous years, the survey included a number of questions on the use of ICT by children aged between 5 and 14. In 2009, the survey asked several questions relevant to child online protection, covering the Internet and mobile phones. The list of Internet problems experienced is shown in Annex 2.

99. The UK Children Go Online Project was undertaken between 2003 and 2005. It involved a face-to-face survey of 1 511 children and young people aged 9-19, together with a survey administered to 906 of their parents.[16] There was also a series of focus group interviews and observations exploring children's use of the Internet. The study is useful because it enabled contrast between the views of children and their parents with regard to online risks and threats. Both the child and parent questionnaires suggest classifications of online threats, as shown in Annex 2.

100. EU Kids Online II will collect information from children about their online experiences. The questionnaire will ask about bullying activities (the child as victim and perpetrator), pornography seen, offline meetings, and sexual messages received and sent.[12]

101. One could also devise classifications based on the severity of risk. In respect of questionnaires, this is likely to be determined subjectively, for example, the YISS-2 youth questionnaire[17] probed the level of distress caused by individual incidents.

Recommendations

102. The recommendations are limited to input classifications of online threats and incidents, that is, classifications that could be included on questionnaires. For analytical purposes, useful output classifications from OECD and *EU Kids Online* were described above.

103. Input classifications of online threats and incidents may differ depending on the data collection methodology and who the respondents are. In Chapter 5, it is suggested that children be asked about online incidents that they have experienced. Because there is a subjective element to this, it is also suggested that surveys ask about threats and incidents that are simple and not open to different interpretation, as well as being policy relevant. Several questions based on those of the UK Children Go Online Survey are provided in Chapter 5.[16]

104. The implied classification is:

Online encounters resulting in offline meetings – whether the child has ever met anyone face to face that s/he first met on the Internet[18]
Pornography – whether the child has ever ended up on a porn site accidentally when looking for something else
Pornography – whether the child has ever received pornographic junk mail by email/instant messaging
Pornography – whether the child has ever been sent porn from someone s/he met on the Internet
Hate sites – whether the child has ever ended up accidentally on a site that was hostile or hateful to a group of people
Violent or gruesome images – whether the child has ever ended up accidentally on a site with violent or gruesome pictures

Children's responses to incidents

105. Some surveys collect information about how children have responded to online threats. For instance, the UK Children Go Online Survey asked children about their responses to the threats, *unwelcome sexual comments* and *nasty or hurtful things*. The questions and set of responses are shown in Annex 2.

106. The YISS-2 youth questionnaire[17] asked a number of response questions as follow up questions on incidents. They included questions on:

- Reactions to requests to send sexual pictures;
- Whether the child had returned to chat rooms where incidents had occurred;
- Whether the child had met online acquaintances in person;
- Whether after incidents, the child or his/her family had installed any blocking, filtering or monitoring software on the computer;
- Whether the child talked to anyone about the incident; and
- Whether the incident was reported to an Internet service provider, the police, or any other place to be investigated.

107. EU Kids Online II will ask children about responses and reactions to bullying, pornographic images, offline meetings and sexual messages.[12]

Recommendations

108. Few surveys appear to have asked about children's responses to an online threat or incident. Examples from the UK Children Go Online Survey child questionnaire and the YISS-2 youth questionnaire are shown in Annex 2. This report does not recommend any particular classification of responses as they are very dependent on the preceding 'incidents' questions. They may also be prone to mis-reporting for reasons discussed in Chapter 5. The EU Kids Online II questionnaire may present a good model for questions about responses. The survey is being conducted during 2010; survey materials and the first findings are expected to be released later in 2010.

Preventive measures

109. A number of guidelines and surveys contain implied classifications of preventive measures. The COP Guidelines for children have proforma contracts for parents and children that are lists of things they promise to do to ensure child safety on the Internet. A number of items on these lists are preventive measures, which can be presented as a classification as follows:[19]

Parent preventive measures (per parent contract)
I will get to know the services and websites my child uses.
I will set reasonable rules and guidelines for computer use by my children and I will discuss these rules and post them near the computer as a reminder.
I will try to get to know my child's "online friends" and Buddy List contacts just as I try to get to know his or her other friends.
I will try to provide close support and supervision of my younger children's use of the Internet, for example by trying to keep their computer in a family area
I will report suspicious and illegal activity and sites to the proper authorities.
I will make or find a list of recommended sites for children.
I will frequently check to see where my kids have visited on the Internet.
I will seek options for filtering and blocking inappropriate Internet material from my children.
I will talk to my kids about their online explorations and take online adventures with them as often as I can.
Child preventive measures (per child contract)
Wherever possible I will choose a safe and sensible screen name for myself that will not broadcast any personal information about my family or me.
I will keep all of my passwords private.
I will discuss with my parents all of the different programmes and applications I use on my computer and on the Internet, and talk to them about the sites I visit. Before I download or load a new programme or join a new site I will check with my parents first to make sure they approve.
When considering signing up to a new online service I will avoid those which demand too much personal information and try to opt for those which ask for less.
I will always take steps to find out what personal information about me will be published by the service by default in my profile and will always opt for the maximum degree of privacy.
I will not share my personal information, or that of my parents or any other family member, in any way, shape or form, online or with someone I meet online. This includes, but is not limited to name, address, telephone number, age or school name.
I will treat others the way I want to be treated.
I will use good manners when I'm online, including good language and respect. I will not pick fights or use threatening or mean words.
I will make my own personal safety my priority, since I know there are some people who might be online and pretend to be someone they're not.
I will be honest with my parents about people I meet online and will tell them, without always being asked, about these people. I won't answer any e-mails or instant messages from anyone my parents have not approved.
If I see or read things that are bad, icky or mean, I will log off and tell my parents so they can try to make sure it never happens again.
I will tell my parents if I receive pictures, links to bad sites, e-mail or instant messages with bad language or if I'm in a chat room where people are using swear words or mean and hateful language.
I will not send anything in the post to anyone I've met online, without my parents' okay. If I get something in the post from someone I've met online, I'll tell my parents immediately (because that means they have my private information).
I will not do anything online that someone asks me to if it makes me feel uncomfortable, especially if I know it's something my parents would not be happy about or approve of.

110. The COP *Guidelines for parents, guardians and educators* suggest a number of actions that could also be used as a classification of preventive measures, as follows:

Parents, guardians and educators	
Safety & security of your personal computer	Keep the computer in a common room
	Install firewall and antivirus software
Rules	Agree house rules about using the Internet and personal devices
	Agree rules for mobile use
Education	Parents should become familiar with the Internet sites used by their children and have a good understanding of how children spend their time online
	Investigate online resources for further information about online safety and how to use the Internet in a positive way
	Understand how children use other personal devices such as mobile phones, games consoles, MP3 players and PDAs
Internet sites features review	Consider whether filtering and blocking or monitoring programmes can help support or underpin children's and young people's safe use of the Internet and personal devices. If you use such software explain what it does and why you are using it to your children. Keep confidential any relevant passwords linked to these programmes. (includes use of filtering and blocking or monitoring programmes)
	Parental consent
	Control use of credit cards and other payment mechanisms
	Ensure age verification is implemented when purchasing goods and services online
	Check if the Internet site uses moderation
	Block access to undesirable content or services
	Check contractual flexibility
	Look at the service scope
	Observe advertising, and report inappropriate advertising
Children's education	Educate your children
	Explain to children to never arrange to meet in person someone they first met online
	Prevent children from sharing personally identifiable information
	Ensure children understand what it means to post photographs on the Internet, including the use of webcams
	Warn children about expressing emotions to strangers
Internet sites safe usage review	Check your child's page or profile
	Ensure children follow age limits of the Internet site
	Ensure children do not use full names
Communication	Communicate with your children about their experiences
Educators	
Safety and security as part of child protection strategies	Use a whole-establishment approach towards responsibility for e-safety
	Develop an acceptable use policy (AUP)
Rules and policies	Sample AUPs are available both online and via local authorities
	Link AUPs with other school policies
	Single point-of-contact
	Need for leadership

Be inclusive	Maintain awareness amongst young people
	Support resiliency
	Encourage disclosure of harms and responsibility taking
Technological solutions	Audit practice
Internet safety policy	Educate teachers on Internet safety policy
	Teach students to never give out personal information when communicating with others
	Require students to search for specific information only
	Preview or test websites before sending links to students

111. A number of household surveys have asked questions about preventive measures. These can be used to construct implied *input* classifications. The surveys are described below, with more information shown in Annex 2.

- Eurobarometer 2008 (Towards a safer use of the Internet for children in the EU – a parents' perspective) asked parents a number of questions on the actions they took to ensure online safety of their children (EC, 2008).
- Eurostat's questionnaire for the 2010 Community Survey on ICT usage in Households and by Individuals includes an Internet security module, which has a question on whether a parental control or a web filtering software is used.
- The UK Children Go Online Project included surveys of children and their parents.[16] The child questionnaire included a number of questions about online security, including appropriate computer software, whether particular sites or activities are blocked or filtered on their home computer, what parents do when the child is on the Internet (e.g. expect you to tell them whenever you go online) and other questions about parents (*e.g.* whether they know how to check which websites the child has visited). Children were also asked about rules.
- The UK Children Go Online parent questionnaire included similar questions, including whether they used the rules that were asked about in the child questionnaire.
- The Australian 2009 survey, Children's Participation in Cultural and Leisure Activities (CPCLA) (ABS, 2009a) asked about actions taken for personal safety and security in home Internet use and mobile phone use.
- The Japanese Telecommunications Usage Trend Survey of 2007 asked households with children under 18 about their use, and awareness of, filtering software (on a PC) and services (on a mobile phone) (Ministry of Internal Affairs and Communications, Japan, 2008).
- The YISS-2 parent questionnaire[20] asks "at any time in the past year, has there been software on the computer your child uses at home that filters, blocks, or monitors what your child does or sees online?" It then asks about various blocking, filtering or monitoring software measures (see Annex 2 for details).
- The EU Kids Online II questionnaire will include some questions asked of children about mediation of parents, peers and teachers, as well as safety advice received from others (including ISPs, websites and the media). Parents will also be asked about preventive actions they take.[12]

112. The COP guidelines for industry also contain a number of recommended actions, which could be used to construct classifications for each industry. Actions that could be (and are) taken by industry are discussed in Chapter 6.

113. A very important aspect of prevention covers the measures employed by governments. The COP guidelines for policy makers contain a number of recommended actions. There are two known surveys directed to governments that ask about policy responses to the problem. The first is the Child Online Protection Initiative National Survey that was run by ITU in 2009 (ITU, 2009g). Apart from the questions on problems (discussed above), the questions constitute a broad classification of preventive measures, with tickbox responses forming the detailed categories (see Annex 2).[21]

114. The second survey directed to governments is the APEC Children Protection Project Survey, which asked member countries open-ended questions about policy responses as shown in Annex 2.

Recommendations

115. As indicated above, and in Chapter 6, there are a large number of potential preventive measures and they can be taken by various actors in the statistical framework. The most common form of measurement is using household surveys to ask questions directed at parents (or other adult respondents) about rules and actions they take to protect children under their care. However, other actors, such as governments, ISPs and children themselves, have also been included in surveys.

116. As discussed in Chapter 6, measurement of preventive actions taken by parents and actions taken by governments seem to be the most likely candidates for creating a set of internationally comparable data. Therefore, classifications dealing with those measures are proposed here.

117. Concerning measures taken by parents, existing questions cover three broad areas: rules for children's Internet use, measures taken by parents at home and use of software. A minimal classification is proposed below (based on questions from Eurobarometer 2008, CPCLA and UKCGO). As with online incidents, options that appear to be simple, not open to interpretation and policy-relevant have been selected. Countries may add to, or further split, the categories using the examples presented above and in Annex 2.[14]

118. EU Kids Online II may present a model for asking children about preventive actions taken by peers and teachers (as well as parents). More information, including results and survey material, will be available from later in 2010.

119. Concerning measures taken by governments, ITU's Child Online Protection Initiative National Survey categories are presented in Annex 2. Subject to further analysis on the usefulness of those categories, it is suggested that they be considered as a classification for the preventive measures of governments in the area of child online protection.

Parents' rules applying to children's Internet use – things that s/he is not allowed to do (at home or elsewhere)
Give out personal information
Buy goods or services online
Talk to people they don't know in real life
Spend a lot of time online
Create a profile in an online community
Use chat rooms
Download movies, videos, images, TV programmes or music
Download or play games
Protective measures taken by parents at home
Placing the computer in a public area of the house
Talking to the child about what s/he is doing or did online
Sitting with your child when s/he is on the Internet
Use of software
Installing Internet filter software on the computer the child uses at home
Installing monitoring software on the computer the child uses at home

Indicator groups

120. It is perhaps helpful to include indicator groupings in a statistical framework. While not necessarily an element of a statistical framework, it could help to visualize the topic in statistical terms. The indicator groups proposed are outlined below and detailed in the chapters following.

Context

121. For this report, context indicators are those that show the background conditions to the subject being measured. Chapter 3 examines a number of context indicators in the following sub-groups.

Internet access and use

122. These indicators use available data to show the extent of, and growth in, Internet access and use. Indicators include Internet subscribers (broadband and narrowband); access to, and use of the Internet by households, individuals and schools; and means of Internet access (including mobile access). Indicators on use of the Internet by individuals can be classified by age, thus giving indicators for children. However, not all countries collect data in respect of children.

Growth of the Web

123. Data include growth in the number of websites, Internet traffic and the growth in registrations on social networking sites.

The subjective aspects of child online protection

124. A number of surveys ask respondents questions designed to gauge subjective information such as their awareness (*e.g.* of Internet risks), their concerns (*e.g.* about those risks) and their attitudes (*e.g.* what should be done about those risks). These subjective elements are examined in detail in Chapter 4.

Children's risk-prone behaviour, incidents and children's responses

125. Perhaps the central areas of measurement for the field, child online protection, is to measure what children are doing that expose them to online threats, what incidents result from that behaviour and how children respond to those incidents. These aspects are examined in Chapter 5.

Preventive actions

126. Preventive measures are examined in Chapter 6. Such measures may be taken at a number of levels and by a number of actors. In this report, we mainly consider preventive measures taken by governments (the policy response) and those taken by children and their parents. The possibility of collecting information from ISPs is also explored.[22]

Data collection models and methods

127. Reflecting the diversity and complexity of the topic, data collection models and methods are varied. The main approaches are outlined below.

Surveys

128. Much of the available data on this topic are collected by surveys of households and individuals. Respondents are usually adults but may be children (though this is less common). Household surveys can be conducted in a number of ways, including face-to-face interview, telephone interview and online. For more information on household surveys on ICT topics, see ITU (2009f).

129. Other surveys include those of governments (two examples are outlined above) and of the ICT sector (for instance, surveys of ISP businesses).

130. Surveys of individuals are often distinguished by whether they are qualitative or quantitative. In some cases, both types are used within an individual study. The differences and merits of each kind of survey have been discussed in several publications, including Lobe *et al.* (2008), EC (2008) and the final report from the Internet Safety Technical Taskforce (2008). The latter explains the differences as follows "Some research questions are better answered by a certain methodology or research design. For example, questions that begin with "why" or "how" are often more adequately addressed through qualitative approaches than quantitative ones. Qualitative scholarship is better suited for providing a topological map of the issues, and quantitative scholarship can account for frequency, correlation, and the interplay of variables."

131. Our main interest in this report is studies that are quantitative, thereby enabling comparison of results over time and between countries. However, smaller qualitative studies that form part of the design of larger scale quantitative surveys may be very valuable (the "combined approach" described by Lobe *et al.*, 2008).

Byproduct data

132. This refers to data collection where statistics are a byproduct of a non-statistical activity. In the area of child online protection, a major activity is that of helplines/hotlines/tiplines. Statistics are available from some of these services. The aim of data collection is to report on the volume and nature of contacts and to focus policy makers on particular problems. While useful information can be obtained from this source, its major failing for statistical purposes is that it is biased. This issue is explored further in Chapter 5, where the use of these sources for measuring incidents is described and assessed.

Other

133. There are various measures of the Internet, including estimates of its size and the number of websites in existence.

Endnotes

[1] EU Kids Online is currently in a second phase which will run from 2009 to 2011, see http://www.lse.ac.uk/collections/EUKidsOnline/. EU Kids Online II includes a quantitative survey across European countries, to be conducted in 2010.

[2] Community Member States and additional European Economic Area countries.

[3] All outputs of the project are available from http://www.lse.ac.uk/collections/EUKidsOnline/Default.htm.

[4] See Lobe *et al* (2008) for a discussion on interviewing children about COP topics.

[5] Conducted by the Crimes against Children Research Center (CCRC) at the University of New Hampshire. The youth questionnaire can be found here http://www.lse.ac.uk/collections/EUKidsOnline/Interview%20schedules/Youthq_YISS2.pdf.

[6] The YISS-2 youth questionnaire can be found here http://www.lse.ac.uk/collections/EUKidsOnline/Interview%20schedules/Youthq_YISS2.pdf.

[7] See Chapter 5 for a discussion on the limitations of such statistics.

[8] Its current members are Eurostat, the International Telecommunication Union (ITU), the Organisation for Economic Co-operation and Development (OECD), the United Nations Conference on Trade and Development UNCTAD, the United Nations Department of Economic and Social Affairs (UNDESA), the United Nations Educational, Scientific and Cultural Organization (UNESCO) Institute for Statistics (UIS), the World Bank, and four United Nations Regional Commissions (the UN Economic Commission for Africa, the UN Economic Commission for Latin America and the Caribbean, the UN Economic and Social Commission for Asia and the Pacific, and the UN Economic and Social Commission for Western Asia). For further information on the objectives and activities of the *Partnership*, see http://www.itu.int/ict/partnership.

[9] For a discussion of the statistical challenges of such classifications, see ITU (2009f).

[10] There are also positive aspects to these activities, though these are not a focus of this report. The final report from the EU Kids Online project (Livingstone and Haddon, 2009b) explores both risks and opportunities associated with Internet use and recommends policies that minimise risks and maximise opportunities.

[11] Online grooming has been described in United Kingdom legislation. Section 15 of the Sexual Offences Act 2003 makes it an offence for "… an adult who has established contact with a child on at least two occasions to meet, or travel with the intention of meeting a child, with intent to commit a sexual offence against that child." See http://www.fkbko.co.uk/root/Parents/cyberwellness/Sexual_health/Grooming1.htm for further information.

[12] Overview of question areas, http://www.lse.ac.uk/collections/EUKidsOnline/Questionnaireoverview1.3.10.pdf.

[13] The last response item, if collected in a dedicated COP survey, could be supplemented with questions on who the content is being shared with. If information about the activities is collected in an ICT household survey, such probing may not be possible.

[14] The advice offered in ITU (2009f) on avoiding bias when splitting or adding categories should be considered.

[15] This is not the exact question wording.

[16] The UKCGO child questionnaire can be found here http://www.lse.ac.uk/collections/EUKidsOnline/Interview%20schedules/UKCGO_ChildQuestionnaire.pdf. The parent questionnaire can be found here http://www.lse.ac.uk/collections/EUKidsOnline/Interview%20schedules/YPNM%20Parent%.

[17] The YISS-2 youth questionnaire can be found here http://www.lse.ac.uk/collections/EUKidsOnline/Interview%20schedules/Youthq_YISS2.pdf.

[18] Such incidents may also be positive. Chapter 5 proposes questions on offline meetings that include an evaluation question on the offline meeting.

[19] Please note the comments earlier in the chapter about some classifications not complying with the rules generally pertaining to statistical classifications.

[20] The YISS-2 parent questionnaire can be found here http://www.lse.ac.uk/collections/EUKidsOnline/Interview%20schedules/Parentq_YISS2.pdf.

[21] The wording has been changed in a number of places to better illustrate the classification inherent in the questions.

[22] A small number of countries run surveys of ISPs. Were this more widespread, then it could be feasible to ask whether they have mechanisms in place to limit children's exposure to Internet threats.

Chapter 3. Child online protection: measuring the context

134. This chapter proposes a number of statistical indicators that describe the context in which online threats to children arise and makes recommendations for a set of statistical indicators that apply across countries. Important elements of the context are growth in Internet access and use, and the proliferation of websites and web content. Useful discussions of the history of the Internet and developments since the early 1990's may be found in ITU (2008).

Internet access and use

135. The work of the Partnership on Measuring ICT for Development was briefly described in Chapter 2. A number of the core ICT indicators defined by the *Partnership* are useful context indicators for child online protection. The core indicators are defined in *Core ICT Indicators* (*Partnership,* 2010). Their availability across countries was described in *Partnership* (2008) and has increased since. At the international level, the data are collected and disseminated by the ITU through its World Telecommunication/ICT Indicators database, and by the UNESCO Institute for Statistics (UIS).

136. The indicators of relevance for this report are in the sets:

- ICT infrastructure and access;
- Access to, and use of, ICT by households and individuals; and
- ICT in education.

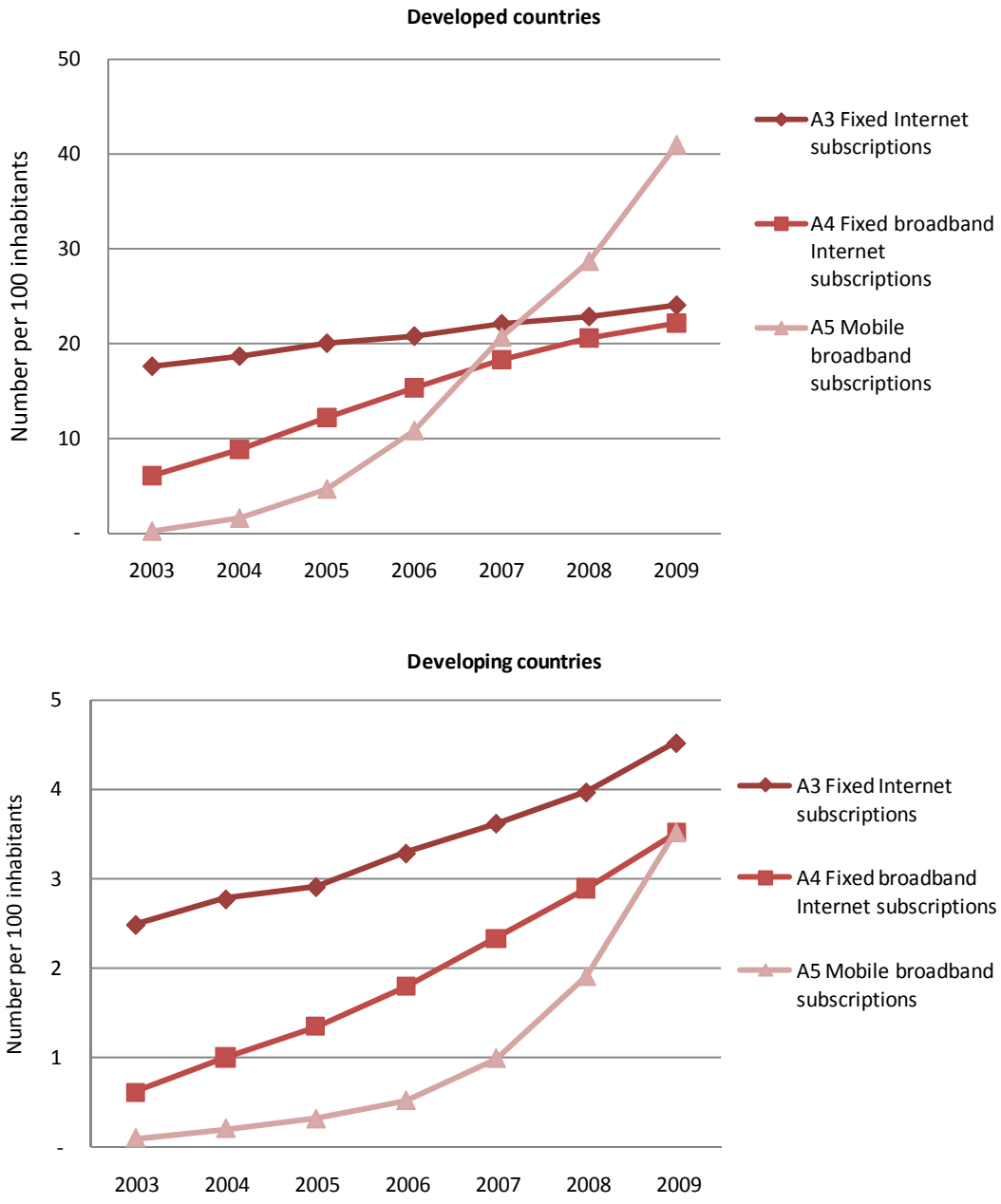
Internet subscriptions

137. Core ICT infrastructure and access indicators A3, A4 and A5 are shown below. They provide a good overview of growth in the number of Internet subscriptions. The data are collected by ITU and are available for a large number of countries.

A3	Fixed Internet subscriptions 100 inhabitants
A4	Fixed broadband Internet subscriptions per 100 inhabitants
A5	Mobile broadband subscriptions per 100 inhabitants

138. Example 1 shows growth over time in the core indicators A3, A4 and A5 for developed and developing countries.

Example 1. Growth between 2003 and 2009: Internet subscriptions (A3, A4 and A5)[1]



Source: ITU World Telecommunication/ICT Indicators database.

Access to, and use of, the Internet by households and individuals

139. The core indicators, HH6, HH7, HH11 and HH12 are shown below. They comprise a basic set of indicators showing access to, and use of, the Internet by households and individuals. The indicators are generally produced by national statistical offices and collected annually by ITU. They are widely available for developed economies and also increasingly available for developing countries – in particular, HH6 and HH7 are available for a reasonable number of developing countries and some least developed countries.

HH6	Proportion of households with Internet access
HH7	Proportion of individuals who used the Internet in the last 12 months
HH11	Proportion of households with access to the Internet by type of access:
	Narrowband
	Fixed broadband
	Mobile broadband
HH12	Frequency of individual use of the Internet in the last 12 months:
	At least once a day
	At least once a week but not every day
	Less than once a week

School access to the Internet

140. The core indicators on ICT in education contain several basic ICT access indicators for schools. Because many children use the Internet at school, it is suggested that ED5, shown below, would be a suitable context indicator. Pilot testing by UIS has shown that the indicator and its categories have reasonable availability across countries.[2]

ED5	Proportion of schools with Internet access by type of access:
	Any Internet access
	Access by fixed narrowband only
	Access by fixed broadband only
	Both fixed narrowband and broadband access

Changes in means of accessing the Internet

141. Internet access is now possible using a variety of devices, including computers (desktops and laptops), handheld computers, games machines, digital TVs and mobile cellular telephones. Increasingly, Internet access is available through mobile access devices and services, and arguably, this trend is making control of children's Internet use more difficult.

142. The set of core ICT indicators include three that show the development towards use of mobile access. They are A5 and parts of HH8, as shown below. OECD (2008) discusses trends towards mobile Internet access and provides some statistics for OECD countries. Many countries collect data on the device that individuals use to access the Internet via their ICT use surveys. They include European countries (through Eurostat's Community Survey on ICT Usage in Households and by Individuals), Singapore (IDA, 2009), China (CNNIC, 2010), Hong Kong (China) (Census and Statistics Department, 2009). Some European countries, China and Singapore produce some data in respect of children.[3]

A5	Mobile broadband subscriptions per 100 inhabitants
HH8	Location of individual use of the Internet in the last 12 months:
	……
	Any place via a mobile cellular telephone
	Any place via other mobile access devices

Children's use of the Internet

143. Data on children's use of the Internet are available for those countries that conduct, and include children within the scope of, household ICT surveys and/or have other relevant collections. Available data may include Internet use by:

- Age
- Gender
- Location
- Activities undertaken
- Frequency of use
- Devices used to access the Internet,[4] and
- Time spent online.[5]

144. ITU (2008) presented data on children's use of the Internet and other ICTs using data from its annual collection of household core ICT indicators and other available sources. Information included Internet and mobile phone use by age and gender, frequency and location of Internet use, and the nature of young people's use of the Internet. Although there were a number of data comparability issues, an interesting picture of children's Internet use emerged (see Example 2).

Example 2. Children's use of the Internet: findings from ITU, 2008

Computer use was higher in both the 5-14 and 15-24 year age groups than the general population in all countries for which data were available. With few exceptions, children (5-14) and youth (15-24) were much more likely to use computers and the Internet than the general population. Use of the Internet in the 15-24 year age group was higher than for the general population in all countries for which data were available.

Rates of use of computers and the Internet for all age groups tended to be lower for transition and developing economies than for developed economies, although there were notable exceptions, for example, Hong Kong (China), the Republic of Korea and Singapore.

Available data indicated similar rates of Internet use for boys and girls aged 5-14 in most countries. The situation was similar in the youth age group of 15-24, although there were more exceptions. For most countries, the situation for the general population was different from that pertaining to young people, with a much higher gender gap in Internet use, in favour of male users.

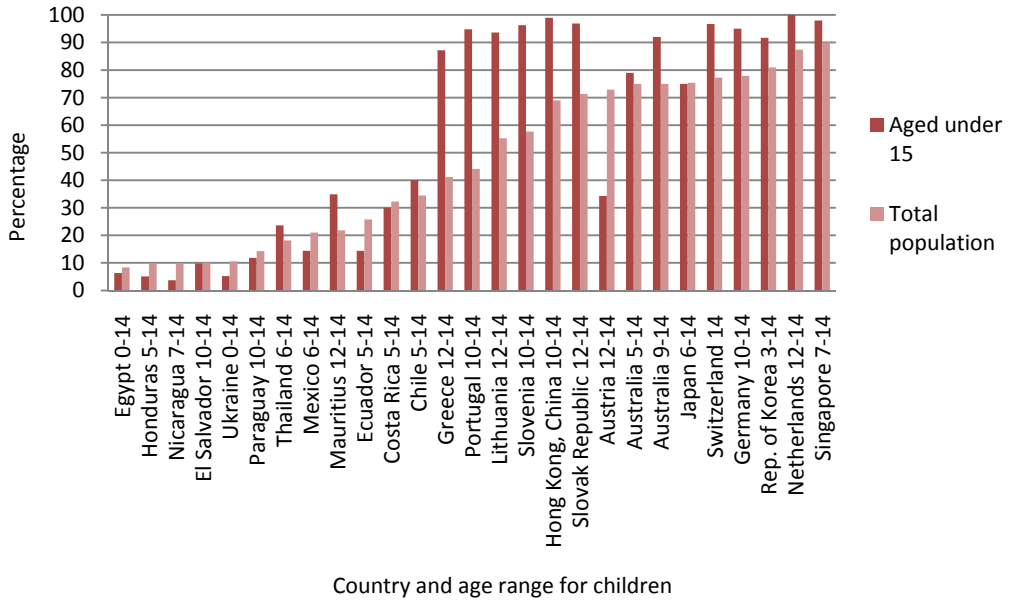
For children and youth in developed economies, home was the most likely location of Internet use. This generally reflected the higher level of home Internet access in developed economies. The more developed Asian economies showed similar patterns of location of use to the developed economies. Among other developing economies, home was less important as a place of Internet use, reflecting lower levels of household Internet access.

Children and youth who use the Internet were quite likely to use it at a place of education. For most economies, children had higher rates of use at a place of education than youth.

Source: ITU, *Use of Information and Communication Technology by the World's Children and Youth: a Statistical Compilation, 2008.*

145. Example 3 shows available data on use of the Internet for children under 15 compared with the total population.

Example 3. Proportion of Internet users, children under 15[6] and total population (HH7)



Source: ITU World Telecommunication/ICT Indicators database, ABS (2009a), Census and Statistics Department, Hong Kong, China (2009), IDA (2009).

146. Of particular relevance to the current topic is the nature of children's use of the Internet. Young people tend to use the Internet in different ways from older people and some of their online activities may be more 'risky' in terms of exposure to threats. Such activities are examined in Chapter 5. Time spent online is a more direct aspect of children's online safety and is also examined in Chapter 5.

147. Suitable context indicators are based on some of the core indicators described above and include use of the Internet by children (HH7), location of that use (HH8) and frequency of use (HH12). While a further split by age and gender would provide useful information, it is unlikely to be feasible for many countries. Many surveys of ICT use ask questions on these aspects of Internet use, although not all include children within their survey scope. For example, the age scope of Eurostat's Community Survey on ICT Usage in Households and by Individuals varies by country, with many European countries unfortunately excluding individuals under the age of 16 from the scope of their national survey.[7]

Growth of the Web

148. Cisco Systems Inc (2009) compiles forecasts of global Internet Protocol (IP) traffic, with the core methodology relying on analyst projections (Internet users, broadband connections, video subscribers, mobile connections, and Internet application adoption). Estimates are split by type of traffic, segment and geography. For a context indicator, we are most interested in the consumer segment, where traffic is split by region and sub-segment (Web/email, File sharing, Internet gaming, Internet voice, Internet video communications, Internet video to PC, Internet video to TV and Ambient video).[8] See Example 4 for examples of forecast data.

Example 4. Growth in global IP traffic

Global Internet Protocol (IP) traffic is projected to quintuple between 2008 and 2013, with a compound annual growth rate of 40%. Regionally, IP traffic is growing fastest in the Middle East and Africa (with a rate of 51%), followed closely by Latin America.

The compound annual growth rate of the consumer segment is 42% between 2008 and 2013. Of the sub-segments, strong growth is projected for the video categories and for Internet gaming. Strong compound annual growth is also projected for all regions, with Africa the highest at 56%.

The compound annual growth rate of mobile data[8] between 2008 and 2013 is estimated at 131%, though is mobile data is very small relative to Internet (in 2008, 33PB compared with 8 126PB).

Source: Cisco Systems Inc (2009).

149. OECD (2009b) describes change in the number of Internet hosts as a leading indicator for measuring growth of the Internet. Surveys are conducted by Internet System Consortium (ISC) of Internet hosts, which are devices connected to the Internet with a unique IP address. Internet hosts include web servers, mail servers and ISP ports. Survey estimates of Internet hosts may underestimate the size of the Internet as they exclude some hosts. OECD (2009b) uses domain name registrations as an indication of the growth in websites. They can be measured as either/both top level domain registrations (for example, *.com*) and country code top level domains (for example, *.com.au*). Between 2000 and 2008, the number of domain name registrations increased six-fold. While data for country code top-level domain registrations are available by country, they may not indicate web growth in that country (as registrations requirements and costs may vary for individual countries, leading registrants to register in another domain).

150. According to web analytics consultant, Antezeta (2010), there are three main ways of measuring website usage and all have limitations. They are:

- User-centric, via measuring what individual users do (*e.g.* what websites they visit);
- Site-centric, measuring how visitors interact with a particular website; and
- Network-centric, collecting data from ISP networks.

151. The Web Analytics Association aims to "… develop common vocabulary, definitions and standards for measuring and reporting web metrics." It has prepared a definitions document (WAA, 2008) that illustrates the complexity of measurement in this area.

152. Not all the website measurement companies have an international scope. Those that do include Alexa, comScore and Nielsen.

153. Alexa provides global web ranking for the top 500 websites (Alexa, 2010). Its rankings for common websites are shown in Example 5. While *Facebook* is ranked number 2 by Alexa overall, it ranks number 1 in Indonesia, Malaysia, the Philippines and Singapore. It ranks number 5 or less in many developed and developing countries. While its ranking is very high in many countries, as a proportion of visits, most countries contribute less than 5 per cent of visits. The US contributes 30 per cent of visitors.

154. According to its website, comScore (2010) employs an Internet panel of over 2 million people from 170 countries and applies harmonized metric definitions, panel recruitment

approaches and data collection methodologies. ComScore data on worldwide unique visitors for December 2009 and January 2010 data were cited by *Facebook* in February 2010 (Facebook, 2010a). The data compared *Facebook*, *MySpace* and *Twitter*. ComScore (2009) reported worldwide *Twitter* growth data between February 2008 and 2009 and visitation broken down by age (the group 25-34 are the highest users). ComScore released global social networking data for June 2007 and 2008 (comScore, 2008) showing year on year growth in unique visitors (15 years and over) by region. See Example 5.

Example 5. Growth in social networking, audience aged 15+, home and work locations, 2007 to 2008

	Unique visitors (thousands)		
	June 2007	June 2008	percentage change
Worldwide	464 437	580 510	25%
Asia Pacific	162 738	200 555	23%
Europe	122 527	165 256	35%
North America	120 848	131 255	9%
Latin America	40 098	53 248	33%
Middle East-Africa	18 226	30 197	66%

Source: comScore World Metrix (comScore, 2008).

155. Nielsen/NetRatings provides ranks of global web parent companies (The Nielsen Company, 2010).[9] These rankings are shown in Example 6. Unique audience ranges for the top 5 sites ranged from 163 to 362 million during January 2010.

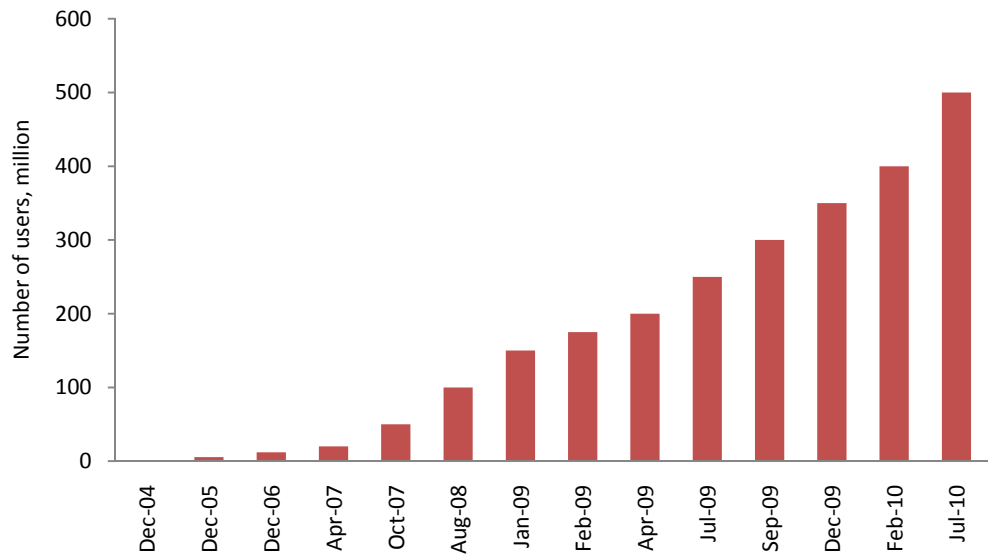
Example 6. Comparison of global rankings of websites, January and February 2010

Site	Alexa	Nielsen
Google	1	1
Facebook	2	4
Youtube	3	Included in 1 (owned by Google)
Yahoo	4	3
Live/Microsoft	5	2
Ebay	23	5
Twitter	12	Not ranked in top 10
MySpace	17	Included with Newscorp (ranked 9)

Source: Alexa (2010), The Nielsen Company (2010).

156. Another way of gauging the growth and prominence of social networking websites is to look at user registration statistics. Facebook's *Company Timeline* (2010b) and *Blog* (2010c) provide information on the number of active users and Example 7 shows the growth in users since its inception in February 2004. Of the active users at March 2010, a quarter (100 million) accessed *Facebook* through mobile devices (Facebook, 2010d).

Example 7. Growth in the number of *Facebook* users, worldwide



Source: Facebook, *Company Timeline* (2010b) and *Blog* (2010c).

157. Facebook (2010e) provided information on the number and growth of users in the US and other selected countries at the start of 2010. For example, according to Facebook, there were 17 million users in Indonesia at 2 January 2010, with a monthly growth rate of 13 per cent. Other high growth rates were observed for India and Thailand (both 12 per cent) and Malaysia (10 per cent).

Recommendations

158. Table 1 below shows the context indicators recommended as part of the set of child online protection indicators. The set consists of indicators that are likely to be both reasonably accurate and reasonably available across countries.[10] It is also useful if they are available as time-series, therefore showing change over time. A number of the sources discussed above, while useful, are not recommended as they do not comply with the conditions of accuracy and availability.

Table 1. Recommended context indicators for child online protection

Indicator	Comments	Source[11]
1.1 Fixed Internet subscriptions per 100 inhabitants, aggregated by level of development (developing/developing countries), time-series (see Example 1)	Partnership core indicator A3	ITU
1.2 Fixed broadband Internet subscriptions per 100 inhabitants, aggregated by level of development (developing/developing countries), time-series (see Example 1)	Partnership core indicator A4	ITU
1.3 Mobile broadband subscriptions per 100 inhabitants, aggregated by level of development (developing/developing countries), time-series (see Example 1)	Partnership core indicator A5	ITU
1.4 Proportion of individuals who used the Internet, last 12 months, by country, children aged under 15 and total population, both by gender, latest data (see Example 3)	Partnership core indicator HH7	ITU
1.5 Proportion of households with access to the Internet by type of access, by country, latest data: - Any Internet access - Narrowband - Fixed broadband - Mobile broadband	Partnership core indicators HH6 and HH11	ITU
1.6 Location of individual use of the Internet, last 12 months, by country, children aged under 15 and total population, by gender if possible, latest data: - Home - Place of education - Community Internet access facility - Commercial Internet access facility - Any place via a mobile cellular telephone - Any place via *other* mobile access devices	Partnership core indicator HH8 (most locations included)	ITU
1.7 Frequency of individual use of the Internet, last 12 months, by country, children aged under 15 and total population, by gender if possible, latest data: - At least once a day - At least once a week but not every day - Less than once a week	Partnership core indicator HH12	ITU
1.8 Proportion of schools with Internet access by type of access, by country, grouped by broad region, latest data: - Any Internet access - Fixed narrowband only - Fixed broadband only - Both fixed narrowband and broadband access	Partnership core indicator ED5	UIS
1.9 Forecast change in Internet Protocol (IP) traffic, current forecast period.[12] (see Example 4) - Global IP traffic by type (Internet, non Internet, mobile) - Consumer Internet traffic by broad region	Indicators of Internet and other IP traffic growth	Cisco Systems
1.10 Change over time in total world number of top-level domain name registrations (global plus country code)	Indicator of global website growth	OECD

Endnotes

[1] Note the different scale on the y-axis of the two charts.

[2] Personal communication with the UNESCO Institute for Statistics, which developed and pilot tested the ICT in education core indicators.

[3] Though they do not all use the term "mobile" in the same way. For instance, China refers to Internet-enabled mobile phones, while other countries tend to interpret it as any way of accessing the Internet that is independent of location *e.g.* using a laptop at a WIFI hotspot.

[4] Of the indicators listed here, this is not part of the core ICT indicator set (although access to the Internet by mobile devices is included as part of core indicator, HH8).

[5] Of the indicators listed here, this is not part of the core ICT indicator set.

[6] The age range for children is shown against the country name. Note that country data are not strictly comparable because of differences in age ranges used in national surveys. Very young children tend to use the Internet less than older children so data for countries with a wide age range will generally be biased downwards. To illustrate this effect, two age ranges are shown for Australia – children aged 5-14 and children aged 9-14. It can be seen that the proportion is lower when younger children are included.

[7] Eurostat separately tabulates results for those aged under 16 where data are provided by participating countries.

[8] Definitions (Cisco Systems Inc, 2009). 'Consumer' includes fixed IP traffic generated by households, university populations, and Internet cafés. 'Mobile' is mobile data and Internet traffic generated by handsets, notebook cards, and mobile broadband gateways.

[9] Definitions, http://en-us.nielsen.com/main/news/news_faqs: 'Unique Audience' includes anyone who went to a site during the reporting period; repeat site visitors are not counted again.

[10] Availability covers the existence of statistics for a particular country and where they do exist, whether they are freely available or a charged product.

[11] These are not necessarily the direct source of the data but are considered to be convenient sources. For instance, ITU compiles indicators using a number of other sources.

[12] The current forecasts (2008-2013) were checked against the previous forecasts (2006-2012) and, for the same years, were reasonably consistent.

Chapter 4. Measuring the subjective aspects of child online protection

159. As Figure 1 in Chapter 2 shows, the subject of child online protection has a number of subjective elements. This chapter discusses the elements of awareness, concerns, attitudes and the perception of harm. These can be briefly described as:

- Awareness and knowledge of online threats by children and parents, and possibly other actors;
- Concerns about online threats by children and parents;
- Attitudes to online threats, preventive measures and available information, by parents and children; and
- Perception of harm caused by the threat, usually from the child's point of view.

Survey data

160. Measuring subjective issues can be very difficult and needs to be approached carefully to avoid statistical bias. A number of surveys have tackled the subjective elements of child online protection, using a variety of approaches. Some of these are discussed below.

Eurobarometer surveys

161. According to the EC, "The quantitative and qualitative Eurobarometer surveys and studies conducted through the Safer Internet Programme are one of the main sources of information concerning the use of online and mobile technologies by children, as well as European citizens' knowledge of ways to protect their children from illegal and harmful content and conduct online."[1]

162. The 2003/2004 survey, *Illegal and harmful content on the Internet* (EC, 2004), was the first on the topic of Internet safety. It measured the attitude and awareness of European Union citizens towards illegal and harmful content on the Internet and their knowledge of how to protect their children against it. For instance, the survey asked parents:

- "Do you feel that you need more information or not about how to protect the children from your household from illegal or harmful content and contact on the Internet?";
- "Would you say that the children in your household know what to do if a situation on the Internet makes them feel uncomfortable?"; and
- Do you know where or to whom you can report illegal or harmful content on the Internet?

163. The 2007 survey, *Safer Internet for children* (EC, 2007), was a qualitative study of 29 European countries covering children aged 9-10 and 12-14. It explored children's perceptions of Internet and mobile phone safety. The study used open-ended questions and language suitable for children (for example, "scary" in relation to risks). It involved a lot of probing and exploration of responses by interviewers.

164. The study had a small sample size and, because of this, as well as its qualitative nature, is more valuable for delivering insights than providing statistical output representative of the population of children.

165. One of the themes was children's perceptions of problems and risks associated with the Internet and mobile phones. Children were given the opportunity to discuss the risks they were aware of ("things that you don't like or find scary") and asked if these problems had changed the way they used the Internet and mobile phones. They were also asked to rate (via coloured stickers) the applications that were most risky. These were then discussed. The interviewers followed this with questions about specific risks, for instance, shocking images and relating with strangers online. The interviewers probed further on several aspects, including what the child would do, how serious they felt the problem to be etc.

166. The 2008 survey, *Towards a safer use of the Internet for children in the EU* (EC, 2008), was a more typical household survey and asked parents about their concerns and awareness of online safety issues. It included questions on concerns about particular online threats ("How worried are you…"); awareness of safety measures ("Which of the following do you think…"); sources of information ("Where do you get your information…"); and, where to report incidents ("Where or to whom would you report illegal content…"). The survey was conducted in 27 EU countries and questions were asked of parents of 6-17 year old children, by telephone interview.

Eurostat surveys

167. The 2010 Eurostat Community Survey on ICT Usage in Households and by Individuals contains an Internet security module. It includes a question on concerns related to Internet use, where one of the categories was "Children accessing inappropriate sites or connecting with potentially dangerous persons from a computer within the household". It also asks whether concerns have prevented some Internet activities, for instance, for example, "Providing personal information to online communities for social and professional networking".

US surveys

168. The US Pew Internet and American Life surveys cover a range of social topics, including how ICT is changing behaviour. The Parents & Teens 2006 Survey (Pew, 2007a) provided a picture of US teenagers' activities online and their concerns about (and management of) some online risks. It asked teenagers who had met a stranger online whether they felt "scared or uncomfortable" because of the online encounter. The survey was conducted by telephone interview, with separate interviews for parents and one of their (randomly chosen) children aged 12-17. A series of focus groups preceded the survey. Other Pew reports are described in Chapter 5.

169. The US Youth Internet Safety surveys (YISS-1 and YISS-2) were conducted by the US Crimes against Children Research Center. The YISS-2 youth questionnaire[2] defined incidents in terms of how the child felt about them, for example:

- "In the past year, did you ever feel worried or threatened because someone was bothering or harassing you online?"

- "In the past year when you were doing an online search or surfing the web, did you ever find yourself in a website that showed pictures of naked people or of people having sex when you did not want to be in that kind of site?
- "How afraid did you feel, on a scale of 1 to 5, with 1 being just a little afraid and 5 being extremely afraid?"

170. The questionnaire also probed awareness of options for reporting incidents. It asked whether the child had heard about a set of options *e.g.* CyberTipline.

171. The US National Teen Internet surveys of 2006 and 2007 (US) conducted by Cox Communications (2007) included questions gauging youth perceptions about the safety or potential risk associated with online activities such as maintaining an Internet profile and posting personal photos.

UK Children Go Online surveys

172. The UK Children Go Online surveys, conducted between 2003 and 2005, measured 9-19 year olds' use of the Internet. Both children and their parents were surveyed and topics included their attitudes, concerns and perceptions of risks. The methodology used a private (self-completion) part of the questionnaire to ask children about exposure to unwanted or inappropriate content (pornography, spam, advertising and violent/racist content).

173. The child questionnaire includes questions probing awareness and concerns, for example, awareness of publicity campaigns on Internet safety and what things children worry about when using the Internet. The adult questionnaire asks about opinions (in terms of their level of agreement to a set of statements) of the Internet, for example, "It's safe for children to spend time on the Internet" and "I am concerned that children might see sexually explicit images on the Internet." The adult questionnaire also probed parents' ability to assist their children, for example, "(Do you) know how to check which websites your child has visited", "(Do you) Know how to access your child's email account".[3]

Recommendations

174. It is clear from the above discussion, that accurate measurement of subjective issues is very challenging. Where international comparability is required, cultural and language issues are additional challenges. It is suggested that subjective aspects of child online protection not be included in a set of internationally standard indicators of child online protection. In general, they are likely to be difficult and expensive to collect, especially where children are the respondents (because of use of open-ended questions and/or a complex sequence of questions) and it is considered unlikely that reliable internationally comparable data would be achievable.

175. Perhaps an exception to this is probing the level of knowledge (awareness) of some aspects of Internet safety. While some questions on this could be open to interpretation, others may be more clearcut, for instance, questions to parents about whether they know how to check which websites their child has visited or whether children are aware that the Internet can be dangerous (both examples are from the UKCGO questionnaires). Some other questions are

country-specific, for example, awareness of agencies to report incidents to *e.g.* a particular national helpline or tipline.

Endnotes

[1] http://ec.europa.eu/information_society/activities/sip/surveys/index_en.htm.

[2] The YISS-2 youth questionnaire can be found here http://www.lse.ac.uk/collections/EUKidsOnline/Interview%20schedules/Youthq_YISS2.pdf.

[3] The UKCGO child questionnaire can be found here http://www.lse.ac.uk/collections/EUKidsOnline/Interview%20schedules/UKCGO_ChildQuestionnaire.pdf. The parent questionnaire can be found here http://www.lse.ac.uk/collections/EUKidsOnline/Interview%20schedules/YPNM%20Parent%.

Chapter 5. Measuring children's risk-prone behaviour, incidents and children's responses

176. This chapter discusses statistics on the types of online behaviour of children that might predispose them to threats (risk-prone behaviours), threatening incidents experienced by children when online, and how they have responded to those incidents. Recommendations are made for data collection on this topic and for a set of statistical indicators that could apply across countries.

Risk-prone behaviour[1]

177. Several studies (reviewed in Internet Safety Technical Taskforce, 2008) have indicated a link between some 'risky' online behaviours and the experience of threatening incidents. However, there are other factors involved, including the characteristics and experience of individual children.[2] Even though these links may not be causal, the level of risk-prone online behaviour may be an indicator of the level of online risk. For the purposes of this report, risk-prone behaviour includes some activities that may increase risk as well as the sheer amount of time spent online. We examine available survey data and social networking website registrations.

Survey data

Children's Internet activities

178. As illustrated in Chapter 3, a number of official country surveys collect data on individuals' Internet activities. Some countries produce such data in respect of children and some ask about activities that are relevant to this report (such as use of social networking sites). However, most countries do not collect much detail. The following surveys include some questions on child online protection (see details on categories in Annex 2):

- As part of the Eurostat *Community survey*, in recent years, European countries have collected data on individuals' use of the Internet to post messages (*e.g.* to social networking sites) and upload content to be shared (Eurostat, 2009b). Some of those countries include children under 16 in the scope of their survey.
- Singapore has a relatively detailed set of ICT activity questions and includes children in its survey (IDA, 2009). Data are produced for a range of relevant activities, covering the Internet generally and portable ICT equipment (*e.g.* mobile phones, PDAs and laptops). Example 8 shows 2008 data for Singapore (IDA, 2009).
- The Australian Bureau of Statistics asked about children's activities in its 2009 CPCLA Survey (ABS, 2009a). Those that could be considered 'risky' are: "Using chat rooms, forums or instant messaging", "Playing online games", "Visiting or using social networking websites – such as *MySpace* or *Facebook*" and "Creating [his/her] own online content such as blogs, websites or uploading photos".[3]

- Thailand, in its 2007 and 2008-09 ICT Household surveys, asked about Internet activities and tabulated the results by age of the user. The categories included "Chatroom & Webboard" and "Game" (National Statistical Office of Thailand, 2007, 2010).
- The Republic of Korea in its 2009 Survey of SNS Usage presented a range of data on individuals' use of social networking services (NIDA, 2009). The survey was conducted in March 2009 and surveyed Internet users, aged 12-49. NIDA defined SNS (social networking service) as "… Internet service that connects users with other users through the Internet, allowing them to build, sustain and manage their social relationships by managing personal network, sharing information, and self expression." The definition includes a wide range of services, including instant messaging, personal networking sites such as *Facebook* and *MySpace*, and virtual reality services such as *Second Life*. Results on SNS usage are available split by type of service, type of activity, gender, age, educational attainment and occupation. Cross-classifications are available showing type of service used by age and by gender (see Example 9 below).
- In 2010, Egypt conducted a pilot survey on Internet safety issues (MCIT, 2010). Information was collected on a number of COP topics, with questions separately asked of children and their parents. A question on risk-prone activities was asked of children and included similar response categories to those shown in Example 8 below.[4]

Example 8. Risk-prone online activities of children and young people, Singapore, 2008

Selected Internet activities	**Internet users, last 12 months, all modes of access**		
	Aged 7-14	Aged 15-24	All residents aged 7 and over
Instant messaging	14%	35%	19%
Social networking sites	11%	30%	14%
Reading blogs created by others	5%	13%	6%
Chat rooms	8%	10%	6%
Creating or maintaining own blogs	5%	9%	4%
Sharing own photos	0%	2%	1%
Broadcasting self-produced videos	3%	10%	6%
Interactive online gaming	29%	19%	11%
Downloading or watching movies, images etc	4%	15%	7%
Selected activities, portable ICT equipment	**Users of portable equipment, last 12 months**		
	Aged 7-14	Aged 15-24	All residents aged 7 and over
Instant messaging	11%	37%	17%
Social networking sites	13%	33%	13%
Reading blogs created by others	5%	17%	6%
Chat rooms	4%	12%	4%
Creating or maintaining own blogs	3%	7%	3%
Sending or receiving digital photograph(s)	3%	6%	4%
Downloading or watching movies, images etc	6%	16%	6%

Source: IDA, Singapore (2009).

Example 9. SNS usage by type, gender and age, Republic of Korea, 2009

Social Networking Service	Gender		Age			
	Male	Female	12-19	20s	30s	40s
Online club/community	57%	56%	63%	72%	51%	41%
Blog/minihompy	52%	57%	62%	75%	49%	34%
Instant messenger	47%	48%	47%	69%	45%	28%
Personal networking site	12%	8%	9%	18%	6%	7%
Virtual reality service	5%	4%	6%	8%	2%	2%

Source: NIDA, Republic of Korea (2009).

179. For more comprehensive information on risk-prone activities, we need to look to non-official sources. Unfortunately, such data are not generally comparable across countries nor available for many countries. However, they provide potential models that a larger set of countries might use.

180. The US Pew Internet and American Life Project was introduced in Chapter 4. Pew reports are based on telephone surveys and, to a lesser extent, focus group studies. Among other things, their reports describe how teenagers use social media (Pew, 2007a,b), how that use is changing (Pew, 2010), how it compares with adult activities (Pew, 2010) and how they manage online identities (Pew, 2007a). The 2009 report, *Teens and sexting*, examined the incidence of teens using mobile phone to send sexually suggestive photos.

181. The reports provide a useful picture of American teenagers' Internet and mobile phone activities, including those that are considered risky for the purposes of this report. Some findings are shown in Example 10.

Example 10. Some findings from Pew surveys, US

Nearly a third (32%) of American online teenagers (and 43% of social-networking teens) have been contacted online by complete strangers and 17% of online teens (31% of social networking teens) have "friends" on their social network profile who they have never personally met (Pew, 2007a).

Of American teenagers aged 12-17 owning cell phones, 4% said they have sent sexually suggestive nude or nearly nude images of themselves to someone else via text messaging, while 15% say they have received such images of someone they know via a text message (Pew, 2009).

Use of social networking websites by American teenagers, aged 12-17, is increasing. In September 2009, 73% of Internet users used social networking websites. This compares with 55% in November 2006 and 65% in February 2008. Among Internet users, teenagers are less likely to use Twitter in 2009 than older people (8% compared with 19%) but are more likely to use social networking sites overall (73% compared with 47%). Teenagers are more likely to create and share content than adults, for example, in 2009, 38% of teens created content compared with 30% of adults (Pew, 2010).

Source: Pew Internet and American Life Surveys.

182. The Crimes against Children Research Center (US) ran studies in 2000 and 2005 on children's Internet safety (Youth Internet Safety Survey – YISS-1 and YISS-2) (Wolak *et al.*, 2006). They conducted telephone interviews with national samples of Internet users aged 10 to 17 and asked about a number of risky activities (see Annex 2 for the list of activities). Some comparable data are available for the two years, 2000 and 2005, enabling valuable measures of change over time.

183. The National Teen Internet surveys of 2006 and 2007 (US) conducted by Cox Communications (2007) had a number of common questions, thus enabling some measures of change over a short time. Respondents were 13-17 year old teenagers and interviews were conducted online. A major objective was to measure online teens' tendency to exhibit potentially risky behavior via the Internet and other forms of virtual communication (such as, text, email, and instant messaging). The study compared the experiences of teens with public online profiles with those without and found that the former face greater exposure to Internet risks (for example, received personal messages from someone they do not know, had been harassed or bullied online).

184. The Eurobarometer 2007 survey, *Safer Internet for children* (EC, 2007), was a qualitative study aimed at children aged 9-10 and 12-14. Among other things, the study asked about various activities, some of which could be considered risky (EC, 2007). The activities are listed in Annex 2.

Time spent online

185. An important aspect of children's online behaviour is the amount of time they spend online. One of the risks identified by the COP initiative is excessive use of the Internet (how the Internet can encourage obsessive behavior or excessive use, which may have damaging effects on children's and young people's health and/or social skills). Several different types of surveys may collect data about the time spent online by individuals. They include time use surveys, ICT use surveys and surveys dealing specifically with child online protection.

186. Time use surveys have been conducted by a large number of countries, including developing countries. The United Nations Statistics Division (UNSD) and the Centre for Time Use Research both document countries conducting time use surveys.[5] UNSD recommends statistical standards for time use surveys, including a time use activity classification, the *International Classification of Activities for Time-Use Statistics*.[6] The only classification of relevance to this report is 1414 – *Using computer technology* (part of Division: 141, Core activities: time spent using mass media). Use of computer technology as a tool for other activities, such as communication, is not included in the UNSD classification. However, at least two countries – Australia, for its 2006 Time Use Survey (ABS, 2008a), and the United Kingdom for its 2005 Time Use Survey (ONS, 2006) – have supplementary codes that indicate whether the Internet and/or a personal computer was used for activities such as communicating. One problem with using time use surveys is that they do not cover all locations in detail and will usually only cover adults (though adults may be as young as 15 or 16).

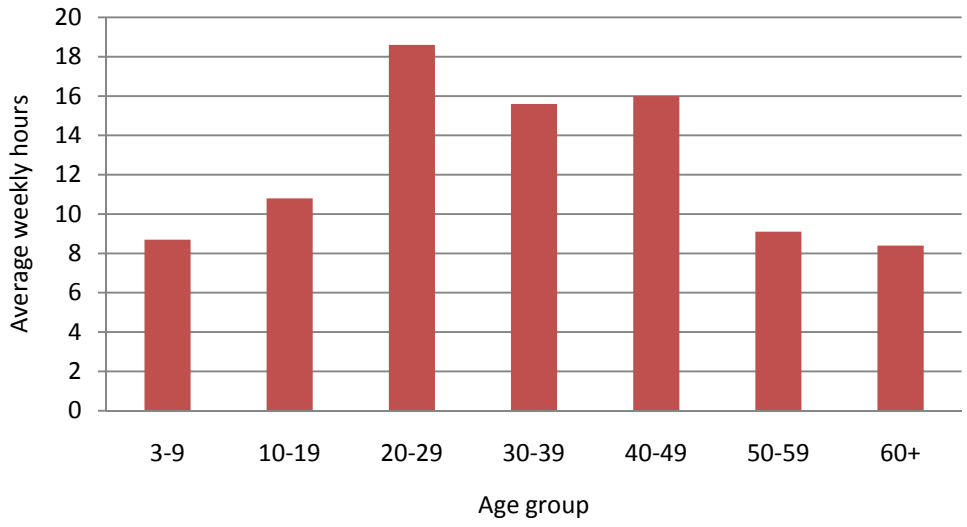
187. While time spent online is not a *Partnership* core ICT indicator, some household ICT surveys include questions on it. For example:

- Australia (usual number of hours per week using the Internet from home, by age range) (ABS, 2009a);
- China (average weekly time online) (CNNIC, 2009);
- Hong Kong (China) (time spent using the Internet per week, by age range) (Census and Statistics Department, 2009);
- Republic of Korea (average weekly time online, by age range) (KISA, 2009); and

- Singapore (average duration of an Internet session, by age range) (IDA, 2009).

188. The five surveys described above all include children. Australia's survey includes children aged 5-14, China covers children aged from 10 years, Hong Kong (China) from 10 years; Republic of Korea from 3 years and Singapore from 7 years. Example 11 shows data from Republic of Korea on weekly average Internet usage hours by age.

Example 11. Weekly average Internet usage hours, by age, Republic of Korea, 2009



Source: KISA (2009).

189. Some child online protection surveys have included questions on the time spent online. They include:

- The US Crimes against Children Research Center 2005 *Youth Internet Safety* Survey (how many hours on a usual day when using the Internet);[7]
- The UK Children Go Online Survey (how much leisure time per day);[8]
- The 2007 Eurobarometer qualitative study, *Safer Internet for children* (how often and how much time) (EC, 2007); and
- The 2010 pilot survey on Internet safety issues conducted by Egypt (MCIT, 2010) used the question and categories recommended in Table 2 of this report. It asked children how many hours, on average, they spent on the Internet per week (<5, 5-10, 11-20, 21-30, 31-40, >40).

Social networking registrations by age of user

190. Given that use of social networking sites[9] by children may be a risky behaviour in terms of online threats, it would be useful to have data on the number of registrations by children for such sites.[10] Unfortunately, such data are generally not publicly available. One exception is Facebook, which provides information on the demographic composition of US users (2010d) (but not for other countries at this stage).[11] At 1 March 2010, 11 per cent of US users were aged 13-17, while 28 per cent were aged 18-25 (the largest group). Only 7 per cent of users were

aged 55 or over. Note that these data will be biased to the extent that users provide false age details when registering.

191. Perhaps a more useful representation of the *Facebook* user data is to look at the proportion of each age group in the whole population who are *Facebook* users. This can be done by comparing the numbers provided by Facebook with population estimates for each group. Results are shown in Example 12.

Example 12. *Facebook* users by age and sex, United States, March 2010

***Facebook* users at 1 March 2010**							
Age/sex	**55-65**	**45-54**	**35-44**	**26-34**	**18-25**	**13-17**	**Total**
Female	4 779 660	8 041 540	10 708 140	12 897 800	15 484 600	6 265 460	58 177 200
Male	2 762 400	5 153 300	8 337 400	10 780 500	14 342 400	5 086 920	46 462 920
Total	**7 542 060**	**13 194 840**	**19 045 540**	**23 678 300**	**29 827 000**	**11 352 380**	**104 640 120**
Proportion of *Facebook* users in each age group (whole population)							
Female	24%	35%	52%	71%	93%	62%	54%
Male	15%	23%	40%	56%	81%	48%	43%
Total	**20%**	**29%**	**46%**	**63%**	**87%**	**55%**	**48%**
***Facebook* growth rates at 1 March 2010, last 28 days, per cent**							
Female	4.6	3.1	2.6	0.9	1.5	4.3	
Male	4.3	3.7	5.6	4.5	3.3	5.8	

Source: Facebook (2010e), US Bureau of the Census population estimates, November 2009, http://www.census.gov/popest/national/asrh/2008-nat-res.html.

192. A Nielsen report from March 2009, provided a breakdown of global[12] growth (December 2007 to December 2008) in *Facebook* unique audience by age (The Nielsen Company, 2009). It showed stronger growth in older age groups for both males and females.

Incidents and responses

Survey data

193. These are generally surveys of children and/or their parents. There is often a subjective element in some of these questions (for instance, a judgement on what content is "harmful").

Eurobarometer surveys

194. The 2005 Eurobarometer survey (*Safer Internet,* EC, 2006) asked parents whether their child had encountered harmful or illegal content on the Internet. An interesting finding is that the proportion reporting 'Don't know' increases with the age of the child.

195. The 2008 survey (*Towards a safer use of the Internet for children in the EU – a parents' perspective*, EC, 2008) was directed to parents of children aged 6-17. Data collected included whether the child had asked for help when they have encountered an Internet problem ("Has

your child ever asked for your help concerning a situation on the Internet that s/he could not handle?).

Eurostat surveys

196. The 2010 Eurostat Community Survey on ICT Usage in Households and by Individuals, in an Internet security module, asked individuals about their experience of Internet threats in the last 12 months, including "Children accessing inappropriate sites or connecting with potentially dangerous persons from a computer within the household".

US, Youth Internet Safety surveys

197. The US Youth Internet Safety surveys (YISS) of 2000 and 2005, asked children aged 10-17 about their experiences of online threats, including sexual solicitation, unwanted exposure to sexual material and harassment via the Internet. A feature of the questions is that they specify that the event was unwelcome, for example:

- "Now I have some questions about things that happen to some young people on the Internet. In the past year, did you ever feel worried or threatened because someone was bothering or harassing you online?"
- "In the past year when you were doing an online search or surfing the web, did you ever find yourself in a website that showed pictures of naked people or of people having sex when you did not want to be in that kind of site?"

198. This highlights that responses on incidents can also be subjective – the responding child must consider how they felt about the incident before responding "yes" or "no". If the encounter or incident did not worry them, then no incident was recorded.

199. The YISS-2 youth questionnaire[7] asked a small number of questions on how the child responded to the incident, for example: "Did this person ever ask you to send them a sexual picture of yourself?" <yes/no/don't know…> then "Did you send a sexual picture of yourself to this person?". More examples are listed in Annex 2.

200. Data from the two YISS studies, showing change over time, are shown in Example 13.

Example 13. YISS: Trends in Online Victimization by Age and Gender, United States

	YISS-1 (2000)	YISS-2 (2005)	Change over time
Youth Internet Users	Rate per 100	Rate per 100	Rate %*
Unwanted sexual solicitations			
All Youth	19	13	-6%
Boys Ages 10 to 13	8	5	–
Boys Ages 14 to 17	15	10	-5%
Girls Ages 10 to 13	15	9	-6%
Girls Ages 14 to 17	34	23	-11%

Unwanted exposure to sexual material			
All Youth	25	34	9%
Boys Ages 10 to 13	16	24	8%
Boys Ages 14 to 17	33	45	12%
Girls Ages 10 to 13	12	21	9%
Girls Ages 14 to 17	29	36	7%
Harassment			
All Youth	6	9	3%
Boys Ages 10 to 13	6	7	–
Boys Ages 14 to 17	6	8	–
Girls Ages 10 to 13	4	7	–
Girls Ages 14 to 17	9	11	–
* Only statistically significant changes are included.			
Source: Wolak *et al.* (2006).			

Australia, Children's Participation in Cultural and Leisure Activities Survey

201. Australia's National Statistics Office, the Australian Bureau of Statistics (ABS), asked about personal safety or security problems associated with the Internet and mobile phones in its 2009 CPCLA Survey (ABS, 2009a). The questions were asked of an adult household member and asked about the type of personal safety or security problems experienced (see Annex 2 for details). The questions were simple and, according to ABS[13] appeared to work well in the field. They were:[14]

"Have there ever been any problems with [Child 1/Child 2/Child 3]'s personal safety or security in [his/her] use of the Internet?" Yes/No/Don't know

"What did the most recent personal safety or security problem involve?

1. Access to inappropriate material[15]
2. Strangers asking for/gaining access to child's personal information
3. Bullying/Threatening behaviour
4. Other"

"Have there ever been any problems with [Child 1/Child 2/Child 3]'s personal safety or security in the use of [his/her] mobile phone? Yes/No/Don't know"

"What did the most recent personal safety or security problem involve?

1. Bullying/Threatening behaviour
2. Strangers asking for/gaining access to child's personal information
3. Receiving inappropriate material in text or media messages
4. Other"

UK Children Go Online surveys

202. The UK Children Go Online surveys of 2003-2005, covered 9-19 year olds' use of the Internet. A national survey was conducted face-to-face with 1 511 children and young people aged 9-19, together with a self-completion survey given to 906 of their parents.[16] The survey asked a number of questions about incidents (see Annex 2 for details). Like the YISS-2 questionnaire, some of the questions required a judgement about the incident, with wording such as ". Unwelcome sexual comments …", "… nasty or hurtful things …". Others were factual, for instance "When on the Internet, have you ever been sent porn from someone you met on the Internet".

203. The UKCGO children's questionnaire is one of the few to ask how the child responded to threats. ("Have you ever received unwelcome sexual comments from someone in any of the following ways?" <email, instant message, text message, chat room> "When this happened what did you do?" <various options> (see Annex 2). Another line of questioning concerned offline meetings: "Have you ever met anyone face to face that you first met on the Internet?" and "Who suggested the meeting?" Follow up questions included whether the child told anyone before attending the meeting, whether they took anyone else with them and how the meeting went.

204. The UKCGO adult questionnaire also asked about online incidents "As far as you know, has your child ever …? (see Annex 2 for options, which include "Been bullied over the Internet" and "Been sent unsolicited sexual material over the Internet").

Republic of Korea, Survey of SNS Usage

205. The 2009 Republic of Korea Survey of SNS[17] Usage (NIDA, 2009) was conducted in March 2009 and surveyed Internet users, aged 12-49. As well as collecting information on usage of social networking services (described above), the survey asked users about their motivation for, and purpose of, using SNS, time spent using SNS, activities using SNS, user perceptions and complaints about SNS.

206. The last topic is particularly relevant to this section and includes problems such as 'Verbal violence or insults', 'Exposure to unwanted risky information' and 'Distribution of inaccurate information'. Users reported their responses to these experiences as including 'Consult/complain/report to service providers', 'Complain directly to alleged wrongdoers' and 'Consult with public complaint handing offices'.

Egypt, pilot survey on Internet safety issues

207. The 2010 pilot survey on Internet safety issues conducted by Egypt (MCIT, 2010) asked children about their experience of online incidents. They included:

- Meeting with strangers face to face following online contact;
- Ending up on a porn site accidentally when looking for something else;
- Receiving pornographic material by email or through pop ups;
- Accidental access to hatred speech and extremist content; and
- Accidental access to bullying content.

Crime statistics

208. Official statistics on crimes committed could be a useful source of data on more extreme online threats. Unfortunately, there appear to be no reliable or comparable sources of such data. There seem to be two main reasons for this.

209. The first, as OECD (2010) has discussed, is variation in national laws. The specificity of legislation in this area varies both with regard to the Internet and to the victims. National laws also vary according to the risks they are addressing, for instance, those relating to content, contact, consumer issues, and privacy/information security.

210. The second reason is the nature of electronic crime as a particular instance of a more general crime. The 2008 *Australian Standard Offence Classification* (ASOC) (ABS, 2008b) discusses electronic crime generally in the context of its statistical crime classification.[18] "Electronic crime rarely represents a specific offence, and often includes a wide range of non-technology linked offences, which can also be committed using electronic means. The behaviour is not necessarily different – this is generally a distinction made based on mode. Where a computer can be used to commit an offence, but has historically been committed without a computer, these offences are coded based on the behaviour of that offence. For example, although child pornography offences can be facilitated by the use of a computer and the Internet, the behaviour associated with the offence remains unchanged based on the mode of production, and the offences should be coded accordingly."

211. Notwithstanding the above, at least one national law enforcement agency collects some data on Internet crimes involving children. Japan's National Police Agency collects statistics on arrests related to child pornography associated with Internet usage and child prostitution via online dating services (National Police Agency, 2010).

212. Another approach to gathering crime statistics is to survey law enforcement agencies. The National Juvenile Online Victimization Study conducted by the Crimes against Children Research Center (CCRC) at the University of New Hampshire, consisted of two waves – the first in respect of 2000 and the second in respect of 2006 (Wolak *et al.*, 2009). Data were collected from a national sample of law enforcement agencies about arrests for (and characteristics of) Internet sex crimes against minors.[19] The survey approach was taken because "Established criminal justice data collection systems do not gather detailed data on such crimes that could help inform public policy and education." Some findings are described in Example 14.

Example 14. Some findings from the National Juvenile Online Victimization Study, US, 2006

"Arrests of online predators in 2006 constituted about 1% of all arrests for sex crimes committed against children and youth."

"…the facts do not suggest that the Internet is facilitating an epidemic of sex crimes against youth. Rather, increasing arrests for online predation probably reflect increasing rates of youth Internet use, a migration of crime from offline to online venues, and the growth of law enforcement activity against online crimes."

"The nature of crimes in which online predators used the Internet to meet and victimize youth changed little between 2000 and 2006, despite the advent of social networking sites."

"Findings from Wave 1 of the N-JOV Study indicated that the stereotype of the online predator who used trickery and violence to stalk, abduct or assault young children was largely inaccurate."

Source: Wolak *et al.* (2009).

Helpline, hotline and tipline statistics

213. Another potentially useful source of data are the *byproduct* statistics generated by helplines and similar on Internet threats and crimes.

214. Child Helpline International (CHI) is an international network of helplines, dealing with crimes against children. CHI collects statistics from its member child helplines around the world and is a member of the COP initiative. Although, at this stage, its statistics do not distinguish Internet-specific crimes, they are considering adding an 'Internet dimension' to their 'reason for contact' field[20] and are testing a question on their 2010 *Violence Against Children* Questionnaire (CHI, 2010).

215. INHOPE is the International Association of Internet Hotlines. Its mission is to eliminate child pornography from the Internet and to protect young people from harmful and illegal uses of the Internet. Although most member hotlines are located in Europe (it covers 21 of the 27 EU member states), other members include Australia, Canada, Iceland, Japan, Russia, South Africa, Korea (Republic of), Taiwan (Province of China) and the United States. INHOPE represents 36 hotlines in 31 countries.[21]

216. Each hotline deals with what is nationally considered to be illegal and this varies between jurisdictions. When a report is received, the material is assessed and traced, then passed to whatever hotline is in the traced host country. The recipient country assesses the alleged infringement under its own laws. If determined to be illegal, the report is referred to the relevant law enforcement officers (INHOPE, 2007).

217. INHOPE collects monthly data from its members. Its *2007 Global Internet Trend Report* provides a rich dataset on hotline reports and outcomes between 2004 and 2006. Data are classified according to the nature of content (see Annex 2), the type of Internet service 'responsible' (*e.g.* websites, email/spam, P2P, FTP, instant messaging, mobile/WAP services) and the type of report (external, derived or proactive). Some INHOPE data are shown in Example 15.

Example 15. INHOPE statistics

Between September 2004 and December 2006, the INHOPE network received 900 000 reports from the public. When added to those proactively found by hotline personnel, the network processed 1.9 million reports. Over 162 000 reports for the whole period were forwarded to law enforcement, more than 150 000 reports to the hosting ISP, more than 170 000 reports to the content owner and almost 33 000 reports to another INHOPE hotline for further processing.

During the last quarter of 2006, the network processed an average of 91 000 reports per month. On average 35 000 reports were received from the public, of which about 19 000 were determined to refer to either illegal or harmful content. An average of 59% of reports referred to content on websites and 30% referred to email/Spam. An average of 9 600 of processed reports per month related to child pornography.

Source: INHOPE (2007).

218. Given that data are collected regularly and according to a consistent statistical framework, it would be tempting to assume that the trends observed reflect those in the real world, therefore, a rise in the number of reports indicates a rise in Internet incidents. For several reasons, that assumption does not hold true. For a start, the network is growing (at an average of one new hotline every three months according to INHOPE, 2007) but it is also becoming more visible and being used by more people. As INHOPE (2007) notes "… The increase in reports could

be due to many reasons …. These reasons could include: change in hotline numbers; change in hotline visibility, change in hotline activity, change in criminal activity, change in visibility of criminal activity."

219. Some individual hotlines also produce data. Of particular interest is the 2009 analysis from Cybertip of Canada (a member of INHOPE) based on public reports submitted between September 2002 and March 2009. The focus was on websites that host child sexual abuse images (Canadian Centre for Child Protection, 2009). While the research was based on reports received from Canadians, it covered websites from all over the world. The report notes that, while the production and distribution of child sexual abuse images is not new, those activities are greatly facilitated by the Internet and other ICTs. The report cites some statistics on the number of websites containing this type of material and contends that it is increasing over time. Data sources cited include studies, Internet filter statistics and the number of sites blocked by individual ISPs. The analysis in the report is based on the 30 000 voluntary reports received from the Canadian public since the inception of Cybertip.ca in 2002. Analysts classified the material in several ways: age and gender of child, severity of the abuse, type of website incident (*e.g.* child pornography), type of website and host country.

220. While the data from the analysis are global – in the same way that the Internet is global – there are several limitations pointed out by Cybertip.ca, for instance:

- The input data are limited to the information received from the Canadian public;
- Cybertip.ca only follows up URLs that have been reported and therefore likely to be readily visible to the public. The content of such sites may be more benign than some more secure content, *e.g.* password protected sites; and
- The content may change before analysts can access it.

Recommendations

Risk-prone behaviour

221. With regard to measuring risk-prone behaviour, it would be relatively easy to specify a small set of potentially risky activities for inclusion in national household ICT surveys. As we saw above, European countries, Australia, Singapore and Thailand already collect some relevant information in their national surveys. Potential issues are that not all such surveys include children and those that do may not ask questions directly of children. Another important issue was raised at the start of this chapter; while risk-prone behaviour may broadly be linked with online incidents, other factors such as individual characteristics are relevant. The identification of 'at-risk' children (apart from by age and gender) would be a desirable classification and may be possible in a dedicated COP survey directed at children.

222. While the surveys of Australia, Singapore, Thailand and Egypt include children, not all European countries include individuals under 16 within their survey scope. It is not known to what extent children are actual respondents in surveys that do include children (they are not respondents in the Australian survey and at least some European surveys).

223. The Partnership on Measuring ICT for Development has included four relevant categories in its 2009 revision of the core ICT indicators (part of HH9, *Internet activities undertaken by individuals in the last 12 months*). Those activities are:

- Purchasing or ordering goods or services;
- Playing or downloading video games or computer games;
- Downloading movies, images, music, watching TV or video, or listening to radio or music; and
- Posting information or instant messaging.

224. It would be very useful to split the last category, per the Eurostat surveys of 2009 and 2010, to "Posting messages to chat sites, social networking sites, blogs, newsgroups or online discussion forums; use of instant messaging" and "Uploading self-created content (text, images, photos, videos, music etc.) to any website to be shared."

225. It could also be useful to split the 'downloading' category to explicitly separate downloading activities (particularly movies and music) from using the Internet as a broadcasting medium (*e.g.* watching TV). The proposed categories are "Downloading movies, videos, images, TV programmes or music" and "Watching TV or video, or listening to radio or music".

226. The ideas inherent in the above questions are relatively simple and also deal with the main risk-prone behaviours of children – communicating online and sharing created content. The other activities dealing with purchasing online, playing computer games and downloading content are also within the scope of COP measurement and can present challenges for children (see discussion of scope in Chapter 2).

227. The Korean Survey of SNS Usage might be a useful model for countries wishing to further explore use of particular social networking services.

228. Regarding measurement of time spent online, it is suggested that the best vehicle for such questions is a national ICT household survey, as such surveys are carried out by a large number of countries and present a relatively simple means of measuring time spent online. Time use surveys are also carried out by a number of countries but are a complicated way of measuring time spent using ICTs because a secondary classification of 'technology used' to carry out a particular activity is required. Such a classification is used by at least two countries (Australia and the United Kingdom) but is not included in the international standards for time use surveys. Time use surveys are also directed towards adults rather than children. For these two reasons they are not recommended for measuring time spent online by children.

229. Specific child online protection surveys are also not recommended as they are not widespread nor carried out within the context of a national statistical system, especially in developing countries. However, they can be a source of ideas for determining the type of time use questions to ask.

230. It is suggested that simple questions on time spent online be used and be directed to children where possible. If that is not possible, then adults should report on their behalf, taking care to answer in respect of Internet use at all locations, not just home. The 2007 questionnaire

from Hong Kong (China) asked "On average, how many hours did you approximately spend weekly using the Internet?". This was split by location and applied to those who had used the Internet at least once a week during the previous twelve months. While it is not suggested that the data be collected by location, a split by location on the questionnaire may result in a more accurate response as it prompts the respondent to include all locations. The Australian CPCLA survey asked "For how many hours per week does [Child 1/Child 2/Child 3] usually access the Internet at home?".[22] The 2007 Eurobarometer survey ascertained time spent online by asking how often the Internet was accessed and then how much time was spent online in a particular session. Many surveys already ask about the frequency of Internet use. While the categories may be too broad to be used in this way, the responses could be a useful check against the number of hours that the respondent reports using the Internet.

231. It is suggested that countries adapt the Hong Kong (China) or the Australian question depending on whether the child him/herself is the respondent. A suitable question, if respondents include children could be:

- "In the last 12 months, how many hours did you usually spend each week using the Internet? (At all locations, including home, work, place of education and Internet cafes)".

232. Where children are not respondents, then the responding adult should be asked about the child's use. The scope of the question should be individuals who have used the Internet in the previous 12 months. The number of hours could be collected as a range rather than an exact number of hours, although neither the Hong Kong (China) nor Australian questionnaires do this. Possibly a reasonable range would be (number of hours per week): <5, 5-10, 11-20, 21-30, 31-40, >40.[23] This range is also recommended for presenting output. An alternative on location is to follow the practice of Hong Kong (China) and ask about each location separately. The locations in the core indicator, HH8 (*Location of individual use of the Internet in the last 12 months*), would be a suitable set. Questions on location of Internet use and weekly hours of use could be linked.

233. Supplementary recommendations are that:

- More countries include children within the scope of their ICT household surveys, thus enabling data on children's risk-prone activity to be more widely available (see ITU, 2009f, Chapter 7 for a discussion on the scope of such surveys).
- Sample sizes be sufficient so that output data for children can be split into smaller age groups, and gender if possible, recognizing the differences in children's behaviour according to age and gender.
- As time series data (showing change over time) are generally more useful than single point-in-time information, it is suggested that countries periodically collect data on risk-prone activities using comparable methodologies and survey questions.

234. While it would be desirable to include an indicator on registrations to (or users of) social networking sites, there does not seem to be good demographic data available across countries. However, the overall growth in *Facebook* registrations has been included as a context indicator (see Chapter 3).

235. Table 2 suggests indicators based on these recommendations.

Incidents and responses

236. This chapter considered several approaches to measuring online incidents. The household survey approach is the more common and likely to be the most useful. For a start, many countries have existing survey vehicles (these would often be ICT household surveys as discussed in the previous section). Secondly, data collected via a survey can be reliably classified by important demographic factors, such as age and gender.

237. We have seen that hotline statistics and crime data are not likely to be able to provide internationally comparable and reliable data, especially over time. Therefore, those approaches are not recommended.

238. It is suggested that any questions on incidents and responses need to be asked of those experiencing the incident/making the response, that is, children. This is a complicating factor for data collection as many ICT household surveys do not collect information from children (although some collect information about children's activities). The reasons for this may be legal and/or ethical. The surveys described above collect such information from children or adults, with a couple of surveys collecting it from both children and their parents. Lobe *et al.* (2008) provide guidance on best practice in the area of interviewing children about COP topics. They also raise the possibility that children could be selected from schools rather than household surveys, though they illustrate some of the problems involved in using such a methodology. However children are selected, it is important for quantitative surveys that the sample be representative of the populations of interest. It may be necessary to adjust data using national benchmarks, as discussed in ITU (2009f).

239. A particular problem when asking children about incidents is that the severity of the incident is a factor of both the nature of the incident and the victim's perception of it. While this element of subjectivity is valuable information, and should be collected if possible,[24] it is doubtful that comparable information could be collected in an international context. It is therefore suggested that questions on incidents and responses be simple, that is, express a single idea, that is not open to interpretation, and have a clear meaning (or at least readily explained on questionnaires or by interviewers). Threats such as online bullying and harassment are likely to be particularly difficult to measure because they are not easily defined and have a subjective element.[25]

240. If we look at the types of survey questions that are both simple and of most policy relevance, there are a small number of examples and they include the following questions (mostly) sourced from the UKCGO child questionnaire:[26]

Online encounters resulting in offline encounters

241. This is a sequence of four questions:

- Have you ever met anyone face to face that you first met on the Internet? Yes/No/I don't want to answer.

- Was the person you met....? (If you have met more than one person that you first met on the Internet, think about the last person you met) Much older than you; A bit older than you; About the same age; Younger than you; I don't want to answer/Don't know.
- Who suggested the meeting? I did; They did; We both did; Don't remember; I don't want to answer/Don't know.
- How did the meeting go? I had a really good time; It was okay, nothing special; I didn't enjoy it; The other person upset me; They turned out to be different from what I expected; We didn't meet after all; I don't want to answer; Other; Don't know.

Pornography

- When on the Internet, have you ever.....? (selection of responses) Ended up on a porn site ACCIDENTALLY when looking for something else? Received pornographic junk mail by email/instant messaging? Been sent porn from someone you met on the Internet? ("Porn" is defined as "… stuff meant for adults. For example, nude people, rude and sexy pictures.")
- Overall, how many times have you seen porn on the Internet? A lot (more than 5 times); A few times; Never; I don't want to answer/Don't know.

Hate sites

- When on the Internet, have you ever.....? Ended up ACCIDENTALLY on a site that was hostile or hateful to a group of people? Yes/No/I don't want to answer/Don't know.

Violent or gruesome images

- When on the Internet, have you ever.....? Ended up ACCIDENTALLY on a site with violent or gruesome pictures (*e.g.* gory or nasty images of people being hurt)? Yes/No/I don't want to answer/Don't know.
- Overall, how many times have you seen violent or gruesome pictures on the Internet? A lot (more than 5 times); A few times; Never; I don't want to answer/Don't know.[27]

242. Few surveys appear to have asked about responses to an online threat or incident. The UK Children Go Online Survey of children and the YISS-2 survey of youth questionnaire are exceptions.

243. The Korean Survey of SNS Usage might be a useful model for countries wishing to further explore incidents and responses arising from use of social networking services.

244. This report does not recommend any particular questions on responses as they are very dependent on preceding questions and likely to be prone to mis-reporting.

245. There are several challenges involved with collecting data from children. They include legal or ethical prohibitions on interviewing children and bias in responses to questions. The latter may arise from the respondent's feelings of shame or embarrassment or the opposite, that is, an inclination to brag about an incident, leading to an exaggerated response. These effects will likely vary by age, by gender and among individuals. While such issues exist for adults as well, they may be magnified for children and, especially, for this subject. It is strongly

recommended that data should be collected from children using personal interviews (either face-to-face or by telephone). The approach of UKCGO, where the interview responses were entered on a laptop and the child was given the laptop to directly enter responses to the more sensitive aspects, should also be considered. Overarching considerations are that interviewers should be sensitive, well-trained and adhere consistently to prompts and procedures.

246. Other aspects of questions put to children, is that they should use language that children understand (*e.g.* use of the "scary" for English-speaking children). Ideally, the reference period should be short enough to avoid recall problems but not so short that only few incidents were reported. In respect of online incidents, UKCGO mostly asks whether something has ever happened, then follows up with questions about the "last time" something happened. The YISS-2 youth questionnaire[28] asks about things that had happened in the last year and then followed up particular incidents. Pew tends to ask respondents about their current activities or whether they have ever done something.

247. Like the other areas covered in this chapter, time series data (showing change in incidents experienced over time) will generally be more useful than single point-in-time information.

248. Table 2 suggests indicators based on these recommendations.

Table 2. Recommended indicators for risk-prone behaviour and incidents

Indicator	Comments	Source
2.1 *Risk-prone behaviour – activities* Proportion of children who have undertaken the following Internet activities in the last 12 months by age group of child (and by gender if possible): - Purchasing or ordering goods or services - Playing or downloading video games or computer games - Downloading movies, videos, images, TV programmes or music - Watching TV or video, or listening to radio or music - Posting messages to chat sites, social networking sites, blogs, newsgroups and other online discussion forums; use of instant messaging - Uploading self-created content (text, images, photos, videos, music etc.) to any website to be shared	The activities are adapted from core ICT indicator HH9, *Internet activities undertaken by individuals in the last 12 months*. The last four are splits of HH9 activity categories – see **Recommendations** above. Availability of data for some of these activities is reasonable.	ITU, Eurostat, individual NSOs
2.2 *Risk-prone behaviour – time spent online* Average time children spent online each week in the last 12 months (hours in ranges: <5, 5-10, 11-20, 21-30, 31-40, >40) by age group of child (and by gender if possible)	Not a core ICT indicator. A similar question is asked in some household ICT surveys. Availability is limited.	Individual NSOs
2.3 *Incidents – online encounters resulting in offline meetings* Proportion of children who have ever met anyone face-to-face that s/he first met on the Internet (classified by age of person encountered compared with the age of the child: much older, a bit older, about the same age, younger), by age group and gender of child if possible**	Very limited availability, would usually be asked on a specialized COP survey rather than an ICT household survey.	The only known sources are the UKCGO study and Egypt's pilot survey.
2.4 *Incidents – pornography* Proportion of children (by age group and gender if possible) who have ever: - Ended up on a porn site accidentally when looking for something else - Received pornographic junk mail by email/instant messaging - Been sent porn from someone you met on the Internet	Very limited availability, would usually be asked on a specialized COP survey. See **Recommendations** above, for definition of 'porn'.	The only known sources are the UKCGO study and Egypt's pilot survey..
2.5 *Incidents and responses – hate sites* Proportion of children (by age group and gender if possible) who have ever: - Ended up accidentally on a site that was hostile or hateful to a group of people	Very limited availability, would usually be asked on a specialized COP survey.	The only known sources are the UKCGO study and Egypt's pilot survey.
2.6 *Incidents – violent or gruesome images* Proportion of children (by age group and gender if possible) who have ever: - Ended up accidentally on a site with violent or gruesome pictures (*e.g.* gory or nasty images of people being hurt)	Very limited availability, would usually be asked on a specialized COP survey.	The only known sources are the UKCGO study and Egypt's pilot survey

Endnotes

[1] There are also positive aspects to the set of risk-prone activities. The final report from the EU Kids Online project (Livingstone and Haddon, 2009b) explores both risks and opportunities associated with Internet use and recommends policies that minimise risks and maximise opportunities.

[2] The Internet Safety Technical Taskforce makes the link between existing characteristics of children and risk of threatening incidents, for example, 'at-risk' youth may be more attracted to environments such as sexually oriented chat rooms. Other characteristics include the level of confidence or familiarity with the Internet.

[3] This survey is conducted every few years, whereas many ICT use surveys are annual. ABS also conducts an annual ICT use survey but it is confined to those aged 15 or above.

[4] For example, Browsing personal mail, Chatting and instant messages, Downloading (music, film, photos, etc), Social networking websites (i.e. Facebook, My Space etc).

[5] See http://unstats.un.org/unsd/demographic/sconcerns/tuse/default.aspx and http://www.timeuse.org/information/studies/.

[6] http://unstats.un.org/unsd/cr/registry/regcst.asp?Cl=231&Lg=1.

[7] The YISS-2 youth questionnaire can be found here http://www.lse.ac.uk/collections/EUKidsOnline/Interview%20schedules/Youthq_YISS2.pdf.

[8] From the UKCGO child questionnaire, which can be found here http://www.lse.ac.uk/collections/EUKidsOnline/Interview%20schedules/UKCGO_ChildQuestionnaire.pdf.

[9] For example, *Facebook*, *MySpace* and *Twitter*.

[10] Such data are of dubious value to the extent that those registering adopt different personas (with different age and/or gender characteristics).

[11] Personal communication, Facebook (February 2010).

[12] Defined by Nielsen for the purposes of the report as: USA, Brazil, United Kingdom, France, Germany, Italy, Spain, Switzerland and Australia.

[13] ABS, personal communication.

[14] ABS CPCLA Questionnaire, April 2009 (unpublished).

[15] Defined by ABS as including "Access to inappropriate websites or web content (regardless of whether the child intentionally or innocently accessed this type of site or content), including pop-ups" and "Receiving emails with inappropriate content".

[16] The UKCGO child questionnaire can be found here http://www.lse.ac.uk/collections/EUKidsOnline/Interview%20schedules/UKCGO_ChildQuestionnaire.pdf. The parent questionnaire can be found here http://www.lse.ac.uk/collections/EUKidsOnline/Interview%20schedules/YPNM%20Parent%.

[17] Social Networking Service.

[18] The ASOC is used in Australian Bureau of Statistics statistical collections, and by the Australian police, criminal courts and corrective services agencies.

[19] Where *Internet-related* is broadly defined to include "… an offender who was a family member, acquaintance, or stranger to a victim used the Internet to communicate with a victim to further a sexual victimization, or otherwise exploit the victim".

[20] CHI, personal communication.

[21] See https://www.inhope.org/. INHOPE was founded under the EC Safer Internet Action Plan and is part funded by the EC Safer Internet Plus Programme.

[22] ABS CPCLA Questionnaire, April 2009 (unpublished).

[23] The suggested ranges are based on time online data from the Hong Kong (China) 2009 survey.

[24] For example, UKCGO follows up the 'porn' question with a question on how the child felt about (e.g. found it interesting, disgusting). YISS-2 used terms like "that you did not want", "threaten or embarrass" to qualify the experiences and probed the level of distress caused by individual incidents.

[25] The final report of the Internet Safety Technical Taskforce (2008) makes the point that "It is difficult to measure online harassment and cyberbullying, because these concepts have no clear and consistent definition. Some definitions include acts that embarrass or humiliate youth while others include only those that are deemed threatening."

[26] The UKCGO child questionnaire can be found here http://www.lse.ac.uk/collections/EUKidsOnline/Interview%20schedules/UKCGO_ChildQuestionnaire.pdf.

[27] This question is not on the UKCGO questionnaire.

[28] The YISS-2 youth questionnaire can be found here http://www.lse.ac.uk/collections/EUKidsOnline/Interview%20schedules/Youthq_YISS2.pdf.

Chapter 6. Measuring preventive actions

249. A very important aspect of child online protection is the action taken to prevent harm to children. This chapter examines available data on this topic and makes recommendations for data collection and for a set of statistical indicators that could apply across countries.

250. Preventive actions may be undertaken by most of the actors outlined in the statistical framework presented in Chapter 2. They include:

- Measures taken by parents and others directly responsible for children's well-being;
- Measures taken by children to protect themselves;
- Government measures in a number of areas; and
- Measures taken by the industry, for example ISPs, social networking websites and search engines.

251. Most of the survey work in this area has been directed at measuring the actions parents take to protect their children. Some surveys have asked children what they do to protect themselves and at least two recent surveys have asked national governments about their policies and measures in this area. These and other measurement approaches are described below.

Preventive measures by parents and children

Survey data

252. Surveys of the measures taken by parents and children are considered together because some studies ask both parents and children similar questions. This can provide an interesting insight into different perspectives.

Eurobarometer surveys

253. The Eurobarometer surveys of recent years have canvassed this topic extensively. The 2003/2004 survey asked about home rules for use of the Internet and other ICTs ("Have you set any rules for him/her about using any of the following either in your household or elsewhere?"). The results indicated a greater level of freedom as children age (EC, 2004). The 2005 survey asked whether filtering/blocking tools for certain websites were applied when the child uses the Internet (EC, 2006). The 2005 survey tabulated information on various preventive measures taken by parents against the age of the child.

254. Eurobarometer 2008 asked parents about the actions they took to ensure online safety of their children (EC, 2008). The relevant questions are shown in Annex 2 and cover actions such as 'staying nearby when child is online' and 'checking the computer later to see which sites the child visited'. The survey also asked about rules for Internet use, such as 'child is not allowed to create a profile in an online community'. Example 16 provides data from Eurobarometer 2008.

Example 16. Eurobarometer 2008: Percentage of parents not allowing at least one activity, EU27	
Giving out personal information	92%
Buying online	84%
Talking to people they don't know in real life	83%
Spending a lot of time online	79%
Creating a profile in an online community	63%
Using chat rooms	61%
Accessing certain websites	49%
Downloading/playing music, films, games	38%
Using email/instant messaging tools	37%
Base: parents whose child uses the Internet, % of "Not allowed"	
Source: Eurobarometer, *Towards a safer use of the Internet for children in the EU – a parents' perspective: summary* (EC, 2008).	

Eurostat surveys

255. Eurostat's questionnaire for the 2010 Community Survey on ICT Usage in Households and by Individuals includes an Internet security module, which has a question on whether a parental control or a web filtering software is used ("Which IT security software or tool do you use?....a parental control or a web filtering software").

Australia, Children's Participation in Cultural and Leisure Activities Survey

256. The CPCLA survey (ABS, 2009a) collected information in respect of children's use of ICT and measures taken to protect children at home from online threats (via Internet and mobile phone). The measures are shown in Annex 2 and, for the Internet, are: placing the computer in a public area of the house, installing an Internet content filter, supervising or monitoring children's Internet use, and educating children about safe and appropriate use of the Internet. ABS tabulated the results by the age range of the child. The Australian survey is unusual in that it collected data on mobile phone use as well as Internet use. The data are theoretically able to be cross-tabulated against whether the child uses the mobile phone to access the Internet. The survey methodology was such that children were not directly asked questions – a responsible adult household member responded on their behalf. The next survey is expected to be run in 2012 and, at this stage, it is envisaged that similar questions will be used.[1]

US, Youth Internet Safety surveys

257. In YISS-2 (2005), parents were asked about use of online safety tools (see Annex 2 for a list). They were described as software that "filters, blocks, or monitors what your child does or sees online".[2]

UK Children Go Online surveys

258. The UK Children Go Online surveys asked both children and their parents about rules and practices for online behaviour.[3] Children were asked about what they are not allowed to do on

the Internet (see list in Annex 2) and what things their parents do to ensure their online safety, for example:

- "When you use the Internet at home, do your parent(s) do any of these things? … Ask/talk to you about what you are doing or did on the Internet";
- "When you use the Internet at home, do your parent(s) do any of these things? … Stay in the same room or nearby when you're online"; and
- "And do they sometimes .....? Sit with you and go online together".

259. Parents were asked similar questions, via a self-completion questionnaire, for instance:

- "Do you (or your spouse/partner) do any of these things nowadays? .... Ask/talk to your child about what he/she is doing or did on the Internet";
- "Do you (or your spouse/partner) do any of these things nowadays? .... Make sure you stay in the same room or nearby when your child is online"; and
- "Do you (or your spouse/partner) do any of these things nowadays? .... Sit with your child and go online together".

260. The contrast between child and parent responses is interesting. In part, it could be caused by children's lack of awareness of their parents' behaviour (for instance, parents may discretely stay nearby when the child is online). Some of the questions were also worded differently, for example, children were asked whether "sometimes" their parents "Sit with you and go online together", while parents were asked if "nowadays" you "Sit with your child and go online together". Some findings are shown in Example 17.

Example 17. UK Children Go Online, What parents do when child is using the Internet

While 25% of children reported that their parents ask what they are doing when using the Internet, 81% of parents reported that they ask what their children are doing.

Similarly, 22% of children reported that their parents stay in the same room or nearby when they are online, compared with 50% of parents reporting that they do that.

The situation was more equal in respect of sitting with the child and going online together (31% of children compared with 32% of parents reporting this). However, note that the question asked of children referred to "sometimes" while that for parents did not. Otherwise, it is possible that children would report a lower incidence of this than their parents.

Source: Livingstone and Bober (2005).

US, Pew surveys

261. In late 2006, Pew conducted a national telephone survey in the United States of just under 1 000 teenager-parent pairs (Pew, 2007a). The parent survey asked about household rules on Internet use by their children and about measures taken at home, including use of filtering software, monitoring software and non-technical measures such as placing the computer in a public area of the home.

262. Among other things, the teenager survey asked about preventive measures taken by teenagers to manage their online identities to maintain privacy. They found that most were taking steps to protect themselves online from obvious sources of risk (such as making contact with strangers). Example 18 provides some findings from this survey.

Example 18. Pew findings US teenagers' management of their online identities, 2006

Two-thirds of teenagers with social network site profiles reported that their online profile is not visible to all Internet users.

Of those whose profile is visible to everyone, nearly half (46%) reported that they give at least some false information on their profiles. This behaviour varied by age and gender, with boys and younger teenagers more likely to post false information on their profiles.

Source: Pew (2007a).

Egypt, pilot survey on Internet safety issues

263. The 2010 pilot survey on Internet safety issues conducted by Egypt (MCIT, 2010) asked both children and their parents about preventive measures. Parents were asked about rules applying to Internet use and used the categories shown in the recommended indicator in Table 3. Parents were also asked about other protective measures, including those in the recommended indicator *Protective measures taken by parents at home* in Table 3.[4]

Measuring the policy response

Survey data

264. There are two known surveys directed to governments that have asked about policy responses to COP. The Child Online Protection Initiative National Survey was run by ITU in 2009; it was conducted online and used tickbox responses (ITU, 2009g). The questions are shown in Annex 2 and responses were grouped according to countries' level of economic development (developed, developing and least developed). According to the designer of the survey (John Carr from the Children's Charities' Coalition on Internet Safety), the survey appeared to work well and produced useful results.[5] As at April, 2010, there were 51 responding countries, including a number of developing and least developed countries.[6] A selection of findings from the survey can be found in Example 19.

Example 19. Some findings from ITU's Child Online Protection Initiative National Survey, 2009

Perceptions of child safety issues in relation to the Internet. Exposure to harmful or inappropriate content was ranked first (mentioned by 80% of countries) while exposure to illegal content was ranked a close second (78% of countries). Just over half (53%) of countries reported that exposure to sexual predators was an issue for them.

The availability of advice or guidance about safer Internet usage by children and young people. Only five countries (10%) reported that such advice was not available in their country. Of areas covered by the advice or guidance, how to deal with or avoid exposure to harmful or inappropriate content was the most common and listed by 80% of respondents, followed by advice and guidance on bullying or harassment (61%), how to report online concerns or incidents (61%) and sexual predators (59%).

Awareness raising and related programmes for parents. Just over half (53%) of the responding countries have such programmes. Most developed countries, but only 20% of least developed countries, reported such programmes.

National focal point or agency with responsibility for promoting Internet safety for children and young people. Just under half (45%) of responding countries have such a focal point.

Legal framework and law enforcement resources. Nearly two-thirds (65%) of countries said that their cyberspace and real world laws in this area were comparable. In most countries (88%), the possession of child pornography/child abuse images is an offence.

Co-operation with the Internet industry. About half the countries reported that they have a hotline or other specific mechanism for reporting suspected illegal content on the Internet and just under half the countries reported that they have such a mechanism for reporting suspected illegal behaviour found or taking place on the Internet.

Help needed by countries. While countries at all levels of development reported that they needed help, calls for assistance from the least developed and the developing countries were strongest.

Source: ITU (2010a).

265. The second survey directed to governments is the APEC Children Protection Project Survey (APEC, 2009), which asked member countries open-ended questions about policy responses (shown in Annex 2). The results for OECD member countries are described by OECD (2010).

Industry measures

Action by social networking websites

266. Social websites may have measures to protect children and are a potential source of data on those measures, which include:[7]

- Minimum age to register accounts;
- Rules and policies to protect younger users from inappropriate contact and content, *e.g.* provision of reporting tools and follow-up of such reports;
- Privacy tools and settings (*e.g.* on *MySpace*, profiles with ages set from 13 to 15 years are automatically private);
- Policies to delete inappropriate user profiles (*e.g.* those that are underage, fake or belong to profiles of registered sex offenders);
- Public education and awareness-raising (*e.g.* Facebook's *Safety Tips*); and
- Software tools (*e.g.* MySpace's *ParentCare* software).

267. Unfortunately, there appear to be limited statistics on the child protection measures taken by MySpace and Facebook. They include an announcement by Facebook in December 2009 of the release of new tools to control information and the subsequent request to its approximately 350 million users to review and update their *Facebook* privacy settings (Facebook, 2010g). Another example is reports on the number of convicted sex offender profiles deleted by MySpace and Facebook.[8]

Action by ISPs

268. ISPs may also take measures to protect children (for instance, by filtering websites or offering parental controls) and are a possible source of statistics on those measures. However, there are a very large number of ISPs in the world and their practices in this area appear to be highly variable. Surveys of ISPs are a possible source of information but are only run by a small number of countries. The Australian Internet Activity Survey, for instance, includes questions on measures taken to protect children. See Example 20.

Example 20. ISPs with over 1 000 active subscribers, selected services offered, Australia, 2007 to 2009

Services offered	Dec 2007	Dec 2008	Jun 2009
Email content filtering services	78%	73%	67%
Web content filtering services	29%	26%	25%

Source: ABS (2009b).

Other actions by the information industry

269. Search engines may have options that limit the websites shown in search results. For example, *Google* has a filtering function called *SafeSearch* that can be set at different levels.[9] Data on the number of sites blocked by such filters would be interesting but appear not to be available. Even if they were, the results may not be a meaningful indicator of the number of suspect sites. The *Google* search works by looking for trigger words in a web page address. This both excludes sites that are not suspect and fails to exclude sites that are suspect but do not indicate that in the name of the web page.[10]

Recommendations

270. Several examples of statistical work in this area have been presented in this chapter. Data on preventive measures may be collected from those doing the protection (parents, governments, businesses) or from those being protected (children).

271. It is suggested that where such data refer to measures taken at home, the data should be collected from the protector (usually parents but respondents in household surveys may be other adults or older siblings). The experience of the UKCGO surveys is that different answers result when parents and children are separately asked about measures taken to protect children. Part of the reason may be that children are not always aware of those measures.

272. Another lesson from the UKCGO survey is that it is useful to collect information on frequency in respect of some preventive measures (for instance, rather than ask whether the parent supervises the child when s/he is using the Internet, it is suggested that questions provide some options on the frequency of the activity, *e.g.* always, often, about half the time, sometimes, never…supervise the child when s/he is using the Internet). As an example, Eurobarometer 2008 (EC, 2008) asked parents about the measures they take when their child uses the Internet at home and asks them to qualify those measures in terms of frequency (always, very frequently, not very frequently, never, don't know/not applicable).

273. Using the tables in Annex 2, we can see that some categories on preventive measures are simple and narrow, that is, there is a single idea and it is clear what it means (or at least could be explained on questionnaires or by interviewers). Many countries conduct a household ICT survey, collecting information on access to ICT (including the Internet) and use of ICTs by one or more household members. Such surveys are suitable for collection of data on household preventive measures and we have seen that some of these surveys already collect such data (for instance, the Eurostat community surveys of 2010 and the Australian CPCLA survey of 2009). It is suggested that questions asking about preventive measures aim to use simple, single-idea categories. Examples that appear to comply with this principle are:

- *Questions to parents on rules applying to children's Internet use*. Eurobarometer 2005 and 2008 include "When your child is online, are there things that s/he is not allowed to do?" Eurobarometer 2008[11] provides a number of options, all of which appear to be simple and relevant. They are: "Spend a lot of time online"; "Access certain websites"; "Create a profile in an online community"; "Use email/ instant messaging tools"; "Use chat rooms"; "Give out personal information"; "Download/play music"; "Download/play films"; "Download/play

games"; "Buy online" and "Talk to people they don't know in real life". Eurobarometer (EC, 2008) tabulated this question as the proportion of parents with Internet-using children. UKCGO had a question on rules in both the parent and children questionnaire. The categories are fairly similar to those of Eurobarometer 2008. Parent data were tabulated as the proportion of parents and children data as the proportion of children. Because of discrepancies in responses between parents and children found by UKCGO (Livingstone and Bober, 2004), it is important that countries are consistent in who they address this question to.

- *Measures taken by parents at home*. These include "Placing the computer in a public area of the house" and "Supervising or monitoring child's use of the Internet" (CPCLA). This can be augmented with other categories: both the Eurobarometer 2008 and *UK Children Go Online* parent questionnaires used a more extensive list than this, including "Make sure you stay in the same room or nearby when your child is online"; "Sit with your child and go online together"; "Help your child when he/she is on the Internet"; "Ask/talk to your child about what he/she is doing or did on the Internet"; "Check the computer later, to see which sites your child visited"; "Check the messages in your child's e-mail account/instant messaging service" and "Check whether your child has a profile on a social networking site/online community". As discussed above, it is useful to have an associated frequency for actions that are ongoing (*e.g.* always, often, about half the time, sometimes, never).
- *Use of software*. Eurobarometer 2008 includes "Does the computer that your child uses at home have installed any of the following software?" with options being "Filtering software (blocking certain websites/activities)" and "Monitoring software (recording where they go/what they do online)". UKCGO asked children and parents very similar questions about filtering and monitoring software. The YISS-2 parent questionnaire[12] asks about "…software on the computer your child uses at home that filters, blocks, or monitors what your child does or sees online", including software that "Filters sexually explicit images or websites"; "Monitors your child's online activities" or "Blocks personal information from being posted or e-mailed". It is not suggested that this level of detail be included on questionnaires. ABS (2009a) asked parents (or a responsible adult) about "Actions taken for personal safety and security in Internet use at home." An option was "Installing an Internet content filter". One of the lessons in ICT statistics is that it is important to define technical concepts. ABS, at least, provides a very detailed definition of an Internet content filter in its instructions to interviewers.[13]

274. Pew (2007a) reported on the preventive actions taken by teenagers to manage their online identities in order to maintain privacy. They found that most teenagers were taking steps to protect themselves online from obvious areas of risk. For example, two-thirds of those with social network site profiles reported that their profile is not visible to all Internet users. This is an example of a single idea with an unambiguous response. Such a question could be a useful inclusion on surveys directed to children (as discussed in the last chapter).

275. Like other areas covered in this publication, time series data (showing change over time) will generally be more useful than single point-in-time information. It is suggested that countries periodically collect data using comparable methodologies and survey questions. This enables some monitoring over time of the preventive actions taken, and may throw some light on the effectiveness of awareness-raising efforts.

276. In addition, it is useful to tabulate the preventive actions taken by parents against the age of the children they are protecting. Several studies have shown that actions differ with the age of the child. For example, Eurobarometer 2006, *Safer Internet* found that parents of young children sit with their child when s/he goes online far more often than parents of teenagers.

277. In respect of governments' activities in child online protection, ITU's Child Online Protection Initiative National Survey is a fairly simple and inexpensive means of providing internationally comparable data (ITU, 2010a). In addition, it is one of the few statistical sources that includes data for a number of developing and least developed countries.[6] There are possible shortcomings of such a survey and they include:

- That a small number of people are responding on behalf of the government (there is room for the contact details of two respondents on the survey form itself). The responding person/persons may not have complete knowledge of all the work of government within the countries. There is also the risk that the respondent/s for one country will interpret some activities as either more or less significant than other respondents. These problems are mitigated to a degree by a statement encouraging countries "… to consult with relevant national stakeholders in order to ensure a comprehensive national overview." and the follow up detail required, for example, "Are there any programmes for parents to help them understand the online safety issues facing their children? Yes/No/Don't know". If "Yes", a number of details are sought including the name of the initiative, organization, dates and contact details.
- That government in a country can consist of several levels (*e.g.* national, provincial and local) and that a response in respect of one level may not apply to the national situation. This is broader problem associated with surveys of government. A partial solution is to specify any limitations of available advice, initiatives, laws or co-operative arrangements with respect to national coverage.
- The relatively low response rate (27% – 51 countries out of 191) poses a risk of non-response bias, that is, that responding countries are different from non-responding countries in terms of how they respond. It is hoped that future surveys can achieve a higher response rate.

278. As measures by government may be very effective, statistics showing change in adoption of such measures over time will be particularly useful in this area.

279. This chapter also looked at the information sector as a source of information but data appear to be limited. While not widespread, surveys of ISPs, such as that conducted by Australia, may provide a good model for individual countries to pursue. However, no recommendations for particular indicators are made in this publication.

280. Table 3 suggests indicators based on the above recommendations.

Table 3. Recommended indicators for preventive actions

Indicator	Comments	Source
3.1 *Parents' rules applying to children's Internet use* Proportion of parents who do not allow children to do certain Internet-related activities (at home or elsewhere) by age group of child (and gender if possible):[14] - Give out personal information - Buy goods or services online - Talk to people they don't know in real life - Spend a lot of time online - Create a profile in an online community - Use chat rooms - Download movies, videos, images, TV programmes or music - Download or play games	Suitable questions could be added to ICT household surveys. They are asked of adult respondents in households where children live. These would preferably be parents, though many surveys only stipulate that an adult respond. Options are from Eurobarometer (2008), with minor adaptation. Availability of data is restricted to EU 27 countries.	Eurobarometer 2008 UKCGO
3.2 *Protective measures taken by parents at home* - Placing the computer in a public area of the house (by age group of child) - Installing Internet filter software on the computer the child uses at home (by age group of child) - Installing monitoring software on the computer the child uses at home (by age group of child) - Talking to the child about what s/he is doing or did online (by age group of child and by frequency: always, often, about half the time, sometimes, never, don't know)[15] - Sitting with your child when s/he is on the Internet (by age group of child and by frequency: always, often, about half the time, sometimes, never, don't know)[15]	Response categories are adapted from CPCLA, UKCGO and Eurobarometer. Note the definitions of Internet filter software and monitoring software (see **Recommendations**). Note also that monitoring and filtering software may be available in the same package. Availability appears to be limited to EU countries, US and Australia. These questions could be included in household ICT surveys.	Eurobarometer 2008, YISS, CPCLA, UKCGO
3.3 *Measures taken by governments* Indicators based on ITU's 2009 COP survey by level of economic development (developed, developing and least developed).	Questions are shown in Annex 2 and several findings are shown in Example 19. No reduction in questions is recommended.	ITU

Endnotes

[1] ABS, personal communication.

[2] The YISS-2 parent questionnaire can be found here http://www.lse.ac.uk/collections/EUKidsOnline/Interview%20schedules/Parentq_YISS2.pdf.

[3] The UKCGO child questionnaire can be found here http://www.lse.ac.uk/collections/EUKidsOnline/Interview%20schedules/UKCGO_ChildQuestionnaire.pdf. The parent questionnaire can be found here http://www.lse.ac.uk/collections/EUKidsOnline/Interview%20schedules/YPNM%20Parent%.

[4] The questions were based on an earlier draft of this report.

[5] Personal correspondence.

[6] Of the responses received, 10 were from developed countries, 31 from developing countries and 10 from least developed countries.

[7] Examples from MySpace (2010), Facebook (2010f). Measures taken by other social networking sites are reviewed in the final report of the Internet Safety Technical Taskforce (2008).

[8] MySpace (http://www.reuters.com/article/idUSN2424879820070724 and http://www.reuters.com/article/idUSTRE51278C20090204?loomia_ow=t0:s0:a49:g43:r1:c1.000000:b30320516:z0) ; Facebook (http://news.cnet.com/8301-13577_3-10168255-36.html).

[9] http://www.google.com/support/websearch/bin/answer.py?answer=35892&hl=en#safe.

[10] These articles explain how the Google filtering works: http://cyber.law.harvard.edu/archived_content/people/edelman/google-safesearch/ and http://news.cnet.com/2100-1032_3-5198125.html.

[11] From the 2008 Eurobarometer questionnaire (annex document), http://ec.europa.eu/information_society/activities/sip/surveys/index_en.htm.

[12] The YISS-2 parent questionnaire can be found here http://www.lse.ac.uk/collections/EUKidsOnline/Interview%20schedules/Parentq_YISS2.pdf.

[13] Defined as follows "Internet content filters are pieces of software that help manage access to online content on home computers by undertaking functions such as blocking, screening or monitoring unwanted material. Such filters allow websites, pop-ups and offensive material to be blocked, emails to be filtered, chat rooms to be monitored and passwords to be set up. Internet content filters can also be individually set for different members of a household. While Internet content filters reduce the risk of accessing unsafe or inappropriate material or sites online, they will not block all offensive content or provide security for the computer itself in the form of keeping out computer viruses." It is possible that other household surveys such as UKCGO and Eurobarometer also have more extensive definitions of technical concepts such as Internet filters available to interviewers.

[14] Choice of options has been determined according to the main actions not allowed per Eurobarometer 2008.

[15] It is suggested that this information be tabulated in two ways, by age group and by frequency. It is unlikely that sample sizes would support a cross-classification of information by age by frequency, even though that would be more useful.

Chapter 7. Statistical challenges

281. This chapter discusses the major statistical challenges in child online protection measurement. Chapter 2 presented a number of elements for a statistical framework and subsequent chapters dealt with measurement of aspects of child online protection. All those chapters have mentioned challenging measurement issues.

282. It should be evident at this point that the nature of the topic *Child online protection* is itself a major statistical challenge. The final report from the Internet Safety Technical Taskforce (2008)[1] found that the risks minors face online are "complex and multifaceted and are in most cases not significantly different from those they face offline". We have also seen, especially in chapters 4 and 5, that many important aspects of the topic are subjective, while others partly rely on an individual's perception or interpretation of a situation.

283. There are a number of other statistical challenges and these are discussed below.

Data availability

284. It is clear that apart from isolated (and usually non-comparable) individual country studies, there is a lack of data on most aspects of child online protection.

285. The exceptions are some existing data on risk-prone Internet activities, time spent online and several pan European surveys conducted by Eurobarometer and, more recently, Eurostat.

286. A particular problem is a general lack of data from developing countries. The level and nature of Internet use tends to be different in those countries – and therefore the problems children face online may differ from those of children in developed countries. As an example, children in developing countries are more likely to use the Internet outside the home (ITU, 2008), thus limiting preventive measures that could be taken by parents.

287. This report has made some recommendations to improve the data available on this topic by proposing relatively small extensions to existing data collection work and suggesting some of the simpler and more objective types of questions that could be included in country household surveys.

International comparability

288. A number of issues hamper the ability to compare child online protection issues across countries. Lack of availability of data, as discussed above, is a major problem. Other issues include differing laws[2] and lack of commonality of definitions and question wording.

289. Several actual and potential data sources with a global reach have been examined in this report and found not to be suitable or available. They include hotline/helpline statistics, crime statistics and data from social networking sites, search engines and ISPs.

290. Probably the best data, for cross-country comparisons, are provided by the Eurobarometer surveys carried out between 2003 and 2008.

291. The *EU Kids Online* final report addressed the challenges of making international comparisons in the context of a number of European studies (Livingstone and Haddon, 2009b; Lobe *et al.*, 2008). It found that a useful approach was to rank the risks and compare that ranking across countries. For example, they found that "Giving out personal information is the most common risky behaviour at around half of online teenagers" and "Seeing pornography online is the second most common risk".

292. The recommendations in this report, if adopted by a large number of countries, should improve international data comparability.

Data interpretation

293. The topic of child online protection can be an emotive one and statistics on the subject need to be interpreted and presented carefully. The final report of the Internet Safety Technical Taskforce (2008), discussed the misleading quotation of 'one-liners' without consideration of the underlying data. They cited the YISS-2 study done at the Crimes Against Children's Research Center (Wolak *et al.*, 2006), which found that quite a high proportion of Internet-using minors (1 in 7) experienced unwanted online sexual solicitation. A closer look at the data shows that 1 in 25 Internet-using minors experienced aggressive online sexual solicitation.

Change over time

294. One of the themes of this report is the value of using a time series of data to show change over time. Such data are of obvious value for monitoring problems and for assessing the effectiveness of policy responses.

295. An important prerequisite for reliable time series data is a consistent measurement approach at all points in time and sample sizes sufficiently large to reliably measure differences between time points. Generally, surveys should be designed to show change over time, in order to produce good estimates of differences between time points. Few of the studies examined in this report have a time series dimension. While there were several Eurobarometer surveys conducted between 2003 and 2008, they were not specifically designed to show change (although a small number of comparisons were made where possible).

296. The YISS-1 and YISS-2 studies were specifically designed to show change between two points in time, 2000 and 2005. The studies used the same methods and asked most of the same questions. In addition, the differences quoted were tested for statistical significance (Wolak *et al.*, 2006).

Data quality

297. There are a number of aspects of data quality that are relevant to any set of statistics. Where data are derived from sample surveys, they include both sampling and non-sampling error.

298. Sampling error is generally higher where sample sizes are small. This is a particular issue for rare events, such as the incidence of the more serious online threats and crimes. It also presents challenges for cross-classification of data, such as by age, gender or socio-demographic status.

299. Non sampling error is also called 'bias' and includes error arising from unrepresentative samples,[3] the sensitive nature of a topic,[4] question wording,[5] interview techniques, processing error and low response rates.[6] It is beyond the scope of this report to examine these sources of error in any detail and readers are referred to publications that cover the subject more completely, including ITU (2009f).

300. The YISS-1 and YISS-2 studies conducted in 2000 and 2005 by the Crimes against Children Research Center at the University of New Hampshire discussed the limitations of their methodologies, in terms of:

- How candid the respondents were, given the sensitive nature of the subject;
- Possible lack of representativeness of respondents ("The young people we did not talk to may have been different from the youth we talked to."); and
- The results are estimates based on a sample and therefore have associated sampling error;

301. In respect of non-survey sources, the biased nature of statistics derived from reporting to hotlines/helplines was discussed in Chapter 5.

Methodology and data collection

302. A good summary of the approaches to measuring child online protection can be found in the final report of the Internet Safety Technical Taskforce (2008) and the final report of *EU Kids Online* (Livingstone and Haddon, 2009b). Data collection in this area of statistics is generally by personal interview (either telephone or face-to-face). While telephone interviewing is likely to be relatively inexpensive, it may not be the best approach for interviewing children. The method of interviewing children used in the UKCGO survey is of interest as it allowed children to directly enter data into a laptop (using computer-assisted personal interview – CAPI – software).

303. In this report, we have discussed examples of data collected from both qualitative and quantitative surveys,[7] and from non-survey sources such as byproduct data (an example of which is hotline/helpline statistics that bring together data collected as part of the reporting process).

304. A very useful guide to best practice in data collection in this area is one of the outputs of the EU Kids Online Project (see Lobe *et al.*, 2008). Advice is offered via a number of FAQs and covers many aspects of surveying in this field, including children as respondents.

305. There are a number of aspects of conducting household surveys that are beyond the scope of this report. ITU (2009f) discusses measurement of household ICT indicators using household surveys and refers to other statistical works in this field.

Endnotes

[1] To the Multi-State Working Group on Social Networking of State Attorneys General of the United States.

[2] A 2006 press release from the International Centre for Missing & Exploited Children illustrates this problem. It refers to a study of child pornography laws in 184 Interpol member countries. The study found that more than half of the countries studied had no laws addressing child pornography and for many other countries, laws were inadequate. See http://www.missingkids.com/missingkids/servlet/NewsEventServlet?LanguageCountry=en_US&PageId=2336.

[3] Samples that are not representative of the population that is in scope of the study. This can be a particular problem when response rates are low.

[4] This report has discussed the problems of bias arising from the sensitive nature of many aspects of child online protection. They include under-reporting through shame or embarrassment and over-reporting by exaggerating or bragging.

[5] This is discussed in the final report from the Internet Safety Technical Taskforce (2008) in connection with a comparison of data from various sources. It may also be a source of error for individual surveys. The use of age-appropriate language, considered earlier in this report, is an aspect of question wording.

[6] Poor response rates are typical of many private surveys (that is, those not conducted by official statistical organisations). Poor response may affect sampling error due to sub-optimal sampling sizes and also non-sampling error, because responses may be biased.

[7] The differences between qualitative and quantitative surveys are explained in Chapter 2.

Chapter 8. Conclusions and summary of recommendations

Conclusions

306. A statistical framework for measuring child online protection (COP) was described in Chapter 2. It included the scope of the COP statistical field, actors and units, concepts and definitions, classifications, relationships between elements, and links to existing statistical frameworks.

307. A number of sources of existing and potential sources of data on COP have been discussed in this report. While there is a general lack of data on the topic, the lack of internationally comparable data and data from developing countries is even more pronounced.

308. Chapter 7 summarized the many statistical challenges inherent in measuring COP and discussed throughout the report. They include: the complex and subjective nature of the subject being measured; lack of data; problems inherent in interpreting COP data; measuring change over time; issues surrounding data quality, both sampling and non-sampling error; methodology and data collection.

Summary of recommendations

309. Recommendations were made in chapters 2 to 6 of this report and are briefly summarized below.

310. A number of existing general and specific statistical standards were examined in Chapter 2. A scope for the COP statistical field was proposed based on the COP guidelines promulgated by ITU. It covers content, contact, children's conduct, commerce, excessive use and societal issues such as the digital divide.

311. Actors and units were generally defined in accordance with the COP guidelines. They are: children (generally, a human being below the age of eighteen years); parents and guardians; educators; governments; industry; perpetrators; and other actors such as NGOs and international organizations.

312. Groups of indicators were recommended as part of the COP statistical framework. They are: background context (*Internet access and use* and *Growth of the Web*); the subjective aspects of child online protection (awareness, concerns etc); children's risk-prone behaviour; incidents and responses; and preventive actions.

313. Existing standards for measuring the background context were described. They include concepts, definitions, classifications, indicators and model questions. It was recommended that they be adopted for the new COP statistical field. Relevant general classifications were also examined and recommended. They include classifications for age, gender and industry.

314. A number of existing classifications and definitions for online safety elements of the framework were presented and discussed. The classifications were distinguished as *output*

classifications (used to present data and as a basis for analysis) and *input classifications* (those applying to input data, *e.g.* appearing on questionnaires). The classifications recommended were generally input classifications and are subsets of the longer classifications presented. They are consistent with the recommendations for the online safety indicators made in chapters 5 and 6. It is suggested that individual countries may wish to collect more extensive data, in which case, more comprehensive classifications would be required.

315. Chapter 3 discussed a number of ways of measuring the context in which online threats to children arise. Two sets of indicators – *Internet access and use* and *Growth of the Web* were suggested and a number of existing indicators were recommended in Table 1 at the end of the chapter. The *Internet access and use* indicators included ITU telecommunications indicators (Internet subscribers and mobile broadband subscriptions) and household ICT indicators (individuals using the Internet and frequency of individual Internet use, and households and schools with Internet access by type of access). The *Growth of the Web* indicators were forecasts to change in Internet Protocol traffic, change over time in total world number of top-level domain name registrations and *Facebook* worldwide active users.

316. Chapter 4 considered what is possibly the most challenging aspect of measuring child online protection, that is, dealing with elements that are highly subjective. They include awareness, concerns, attitudes and the perception of harm, and involve parents and children. Attempts to measure these aspects were described and the challenges highlighted. Given the uncertainty of measuring such elements in an international context, no recommendations were made for indicators, although it was suggested that simple questions about knowledge or awareness could be added to country questionnaires. Some questions of this type may be country-specific, for example, whether the respondent knows which agencies to report incidents to or has heard of particular organizations that are active in prevention.

317. Chapter 5 discusses the online safety elements of children's risk-prone behaviour, online incidents and children's responses to those incidents. A number of potentially useful types of data sources were examined including survey data, crime statistics, social networking site data, and data from helpline reports. Ultimately, survey approaches were recommended for measuring these aspects of child online protection.

318. With regard to measuring risk-prone behaviour, a small set of potentially risky activities was identified, based on the existing Internet activities categories of the Partnership's indicator HH9, *Internet activities undertaken by individuals in the last 12 months.* Sources for measuring time spent online were also examined and recommendations for data collection made. Supplementary recommendations were that the scope of existing ICT household surveys be expanded to include children, where they do not already; that samples are of sufficient size to provide output by children's age and gender; and that such surveys be periodically conducted so that time series data are available.

319. For incidents and responses, it was suggested that children (rather than parents) be asked about incidents that had occurred to them, and their responses to those incidents. It was further suggested that questions on incidents and responses have a single clear idea, that is not open to interpretation, and that language appropriate for children be used. A set of simple and relevant questions for inclusion on surveys was suggested and cover online/offline encounters,

pornography, hate sites, and violent or gruesome images. As above, it was suggested that time series data be collected where possible.

320. The recommendations on incidents do not cover all the types of incidents that might be experienced, for instance they exclude bullying and harassment, which are not easily defined and have a subjective element. Nor do they cover questions on children's responses (although possible models were presented).

321. Chapter 5 concludes with a table showing indicators for risk-prone behaviour and incidents (Table 2). They cover a set of Internet activities that may be undertaken by children and appear to increase their risk of harm; the time spent online by children; and a set of incidents that appear to be measurable in a cross-country context.

322. Chapter 6 looked at measuring preventive actions by several types of actors in the COP framework. It ultimately focused on the actions of parents and governments and recommended survey approaches in both cases. As with other indicators, it was suggested that time series data be collected where possible.

323. Existing ICT (or other) household surveys may be used for measuring the actions of parents and three types of questions were suggested: rules applying to children's Internet use, measures taken by parents at home, and use of software.

324. ITU's Child Online Protection Initiative National Survey appears to be a reasonable model for collecting internationally comparable data on preventive measures taken by governments. Possible shortcomings and partial solutions were discussed.

325. Chapter 6 concludes with a table showing recommended indicators of preventive actions (Table 3). They cover parents' rules applying to children's Internet use; protective measures taken by parents at home; and measures taken by governments. The first two sets of indicators are likely to be collectable using ICT household surveys, while the third consists of information from a COP survey of governments conducted by ITU.

326. Annex 1 brings together the indicators recommended in the report. This list of indicators could be used by countries in their initial efforts to collect internationally comparable data on child online protection.

Annex 1: Recommended indicators for child online protection

This annex brings together the recommended indicators from tables 1-3. It covers context, children's risk-prone behaviour and incidents, and preventive actions. See tables 1-3 for more detailed information, for instance, on data availability and data sources.

Recommended context indicators
1.1 Fixed Internet subscribers per 100 inhabitants, aggregated by level of development (developing/developing countries), time-series
1.2 Fixed broadband Internet subscribers per 100 inhabitants, aggregated by level of development (developing/developing countries), time-series
1.3 Mobile broadband subscriptions per 100 inhabitants, aggregated by level of development (developing/developing countries), time-series
1.4 Proportion of individuals who used the Internet, last 12 months, by country, children aged under 15 and total population, both by gender, latest data
1.5 Proportion of households with access to the Internet by type of access, by country, latest data: - Any Internet access - Narrowband - Fixed broadband - Mobile broadband
1.6 Location of individual use of the Internet, last 12 months, by country, children aged under 15 and total population, by gender if possible, latest data: - Home - Place of education - Community Internet access facility - Commercial Internet access facility - Any place via a mobile cellular telephone - Any place via *other* mobile access devices
1.7 Frequency of individual use of the Internet, last 12 months, by country, children aged under 15 and total population, by gender if possible, latest data: - At least once a day - At least once a week but not every day - Less than once a week
1.8 Proportion of schools with Internet access by type of access, by country, grouped by broad region, latest data: - Any Internet access - Fixed narrowband only - Fixed broadband only - Both fixed narrowband and broadband access
1.9 Forecast change in Internet Protocol (IP) traffic, current forecast period. - Global IP traffic by type (Internet, non Internet, mobile) - Consumer Internet traffic by broad region
1.10 Change over time in total world number of top-level domain name registrations (global plus country code)

Recommended indicators for risk-prone behaviour and incidents
2.1 *Risk-prone behaviour – activities* Proportion of children who have undertaken the following Internet activities in the last 12 months by age group of child (and by gender if possible): - Purchasing or ordering goods or services - Playing or downloading video games or computer games - Downloading movies, videos, images, TV programmes or music - Watching TV or video, or listening to radio or music - Posting messages to chat sites, social networking sites, blogs, newsgroups and other online discussion forums; use of instant messaging - Uploading self-created content (text, images, photos, videos, music etc.) to any website to be shared
2.2 *Risk-prone behaviour – time spent online* Average time children spent online each week in the last 12 months (hours in ranges: <5, 5-10, 11-20, 21-30, 31-40, >40) by age group of child (and by gender if possible)
2.3 *Incidents – online encounters resulting in offline meetings* Proportion of children who have ever met anyone face-to-face that s/he first met on the Internet (classified by age of person encountered compared with the age of the child: much older, a bit older, about the same age, younger), by age group and gender of child if possible
2.4 *Incidents – pornography* Proportion of children (by age group and gender if possible) who have ever: - Ended up on a porn site accidentally when looking for something else - Received pornographic junk mail by email/instant messaging - Been sent porn from someone you met on the Internet
2.5 *Incidents and responses – hate sites* Proportion of children (by age group and gender if possible) who have ever: - Ended up accidentally on a site that was hostile or hateful to a group of people
2.6 *Incidents – violent or gruesome images* Proportion of children (by age group and gender if possible) who have ever: - Ended up accidentally on a site with violent or gruesome pictures (*e.g.* gory or nasty images of people being hurt)

Recommended indicators for preventive actions
3.1 *Parents' rules applying to children's Internet use* Proportion of parents who do not allow children to do certain Internet-related activities (at home or elsewhere) by age group of child (and gender if possible): - Give out personal information - Buy goods or services online - Talk to people they don't know in real life - Spend a lot of time online - Create a profile in an online community - Use chat rooms - Download movies, videos, images, TV programmes or music - Download or play games
3.2 *Protective measures taken by parents at home* - Placing the computer in a public area of the house (by age group of child) - Installing Internet filter software on the computer the child uses at home (by age group of child) - Installing monitoring software on the computer the child uses at home (by age group of child) - Talking to the child about what s/he is doing or did online (by age group of child and by frequency: always, often, about half the time, sometimes, never, don't know) - Sitting with your child when s/he is on the Internet (by age group of child and by frequency: always, often, about half the time, sometimes, never, don't know)
3.3 *Measures taken by governments* Indicators based on ITU's Child Online Protection Initiative National Survey by level of economic development (developed, developing and least developed).

Annex 2: Examples of measurement categories used in child online protection surveys and output

Children's risk-prone behaviour

Eurobarometer 2007 Survey (Safer Internet for children)

Internet applications
Searching for information as a part of my school work
Searching for information on subjects which interest me/surfing for fun
Sending and receiving emails
Using instant messaging (MSN)/chatting with friends
Engaging in open chatrooms
Creating my own blog/homepage and posting my own texts, photos, music on the Internet
Reading and responding to friends' blogs/homepages
Reading and responding to blogs/homepages of someone I have never met
Playing on-line games
Downloading music, films, videos, games or other files
Sharing files (music, films, videos, games or others)
Sharing photos
Downloading ring tones/images for my mobile phone
Taking part in competitions
Making phone calls through the Internet
Mobile phone applications
Making and receiving phone calls
Sending/receiving SMSs
Taking photos/images
Sending/receiving/sharing images
Connecting to the Internet through my mobile phone

Eurostat, Community Survey on ICT Usage in Households and by Individuals, 2009 and 2010

Selected Internet activities
Posting messages to chat sites, social networking sites, blogs, newsgroups or online discussion forum, use of instant messaging
Uploading self-created content (text, images, photos, videos, music etc.) to any website to be shared

Crimes against Children Research Center, Youth Internet Safety Survey, 2005 (YISS-2), children's questionnaire

The number of times (in the past year) the child posted:
his/her real last name, phone number, school name or home address where anyone online could see it (like in a profile or online journal)
his/her age or year of birth online where anyone online could see it
a picture of him/herself on the Internet where anyone online could see it
Whether (in the past year) the child:
posted a sexual picture of him/herself online
used a screen name that s/he considered sexual in any way
The number of times (in the past year) the child:
gave his/her real last name, phone number, school name or home address to someone s/he met online but had never met in person
gave his/her age or year s/he was born to someone s/he met online but had never met in person
has sent a picture of him/herself over the Internet to someone s/he met online who s/he had never met in person, including through a web cam

Singapore (IDA), Annual Survey on Infocomm Usage in Households and by Individuals, 2008

Selected Internet activities
Instant messaging
Social networking sites
Reading blogs created by others
Chat rooms
Creating or maintaining own blogs
Sharing own photos
Broadcasting self-produced videos
Interactive online gaming
Downloading or watching movies, images etc
Selected activities, portable ICT equipment
Instant messaging
Social networking sites
Reading blogs created by others
Chat rooms
Creating or maintaining own blogs
Sending or receiving digital photograph(s)
Downloading or watching movies, images etc

Australia (ABS), Children's Participation in Cultural and Leisure Activities Survey, 2009

Selected Internet activities
Does the child access the Internet at home for
Emailing?
Using chat rooms, forums or instant messaging?
Playing online games?
Listening to or downloading music?
Watching or downloading TV programmes, videoclips, cartoons or movies – for example on YouTube?
Using eBay, auction sites or Internet shopping?
Visiting or using social networking websites – such as MySpace or Facebook?
Creating [his/her] own online content such as blogs, websites or uploading photos?

Online threats and incidents

INHOPE classification of reports of potentially illegal or harmful content

Reports of potentially illegal or harmful content	**Definition**
Child Pornography	Child pornography under national law
Other Child-Related Content	Child trafficking, child sex tourism, child nudism, child grooming activities, child erotica/inappropriate images of children, and adult pornography accessible to children
Racism and Xenophobia	Racism or xenophobia under national law
Extreme Adult Content	Extreme sexual and physical violence, non-consensual sexual acts and other types of pornographic content deemed illegal under national law. For example, rape websites etc.
Adult Pornography	Pornographic content that in most countries does not contravene national law.
Other Illegal Content	Promoting violence against an individual, terrorism and drugs.
Reports not considered to be illegal or harmful	
SPAM not Containing Illegal Content	
Other Content	

ITU's Child Online Protection Initiative National Survey, 2009, problems

What are the main problems facing children and young people in your country in relation to the Internet: [Please tick as many as apply]
Exposure to illegal content
Exposure to other forms of harmful/inappropriate content
Exposure to bullying or harassment
Exposure to sexual predators
Exposure to travelling sex offenders (sex tourism)
Exposure to fraud and/or financial scams
Exposure to identity theft
Over-use or "addiction" to the technology
Exposure to Internet related crime such as virus attacks/hacking
Exposure to age-inappropriate commercial activity
There are no problems. Everything seems to be fine
Don't know/Other (If other, please specify)

Eurobarometer 2008 (Towards a safer use of the Internet for children in the EU – a parents' perspective), Internet situations that children could not handle

Has your child ever asked for your help concerning a situation on the Internet that s/he could not handle? Yes/no
What was the situation in which your child asked your help:
A technical problem (like a virus)
Being harassed online
Information searching
Being bullied online
Being contacted by strangers online
Having found sexually or violently explicit images online
Something else

Crimes against Children Research Center, Youth Internet Safety Survey, 2005 (YISS-2), children's questionnaire, incidents and activities

Unwanted sexual exposure and solicitation
Did anyone use the Internet to threaten or embarrass you by posting or sending messages for other people to see?
Did you find yourself in a website that showed pictures of naked people or of people having sex when you did not want to be in that kind of site?
Did you receive email or Instant Messages that you did not want with advertisements for or links to x-rated websites?
Did you open a message or a link in a message that showed you actual pictures of naked people or of people having sex that you did not want?
Did you find people talking about sex in a place or time when you did not want this kind of talk?
Did anyone on the Internet ever try to get you to talk online about sex when you did not want to?
Did anyone on the Internet ask you for sexual information about yourself when you did not want to answer such questions?
Did anyone on the Internet ever ask you to do something sexual that you did not want to do?
Did anyone on the Internet ever ask you or encourage you to runaway from home?
What the child was doing when these incidents occurred
Using an email account (includes opening a file)
At an online dating or romance site
In a chat room
Using instant messages
In a game room or other game site
At an online forum or message board
At another specific web page or website
Using downloads from file sharing programmes
In an online journal or blog

Australia (ABS), Children's Participation in Cultural and Leisure Activities Survey, 2009, Internet problems experienced

Problems with child's personal safety or security in [his/her] use of the Internet
(What did the most recent personal safety or security problem involve?)
Access to inappropriate material
Strangers asking for or gaining access to child's personal information
Bullying or threatening behaviour
Other

UK Children Go Online children survey, 2003-2005, children's questionnaire, threats

Questions asked of children
Have you ever received unwelcome sexual comments from someone in any of the following ways <email, instant message, text message, in a chat room>?
Has someone ever said nasty or hurtful things to you in any of the following ways <email, instant message, text message, in a chat room>?
When on the Internet, have you ever.....?
Ended up on a porn site ACCIDENTALLY when looking for something else
Visited a porn site ON PURPOSE
Seen a pop-up advert for a porn site while doing something else
Received pornographic junk mail by email/instant messaging
Been sent porn from someone you know
Been sent porn from someone you met on the Internet
When on the Internet, have you ever.....?
Ended up ACCIDENTALLY on a site with violent or gruesome pictures (*e.g.* gory or nasty images of people being hurt)
Visited a site with violent or gruesome pictures ON PURPOSE
Ended up ACCIDENTALLY on a site that was hostile or hateful to a group of people
Visited a site that was hostile or hateful to a group of people ON PURPOSE
Questions asked of parents
As far as you know, has your child ever …?
Visited an Internet chat room
Made new friends over the Internet
Been bullied over the Internet
Received unwanted sexual comments over the Internet
Come across pornography on the Internet
Been sent unsolicited sexual material over the Internet
Come across violent or gruesome material on the Internet
Come across racist or hateful material on the Internet
Met someone face to face that they first met on the Internet
Given out information that they shouldn't on the Internet

Children's responses to incidents

UK Children Go Online children survey, 2003-2005, children's questionnaire, responses to threats

Questions
Have you ever received unwelcome sexual comments from someone in any of the following ways? <email, instant message,
Has someone ever said nasty or hurtful things to you in any of the following ways? <email, instant message, text message,
Responses
I deleted it straight away
I tried to block messages from the person
I told a parent
I told a friend
I replied to the message to ask them to stop
I replied to the message to send sexual comments/nasty comments to them
I don't want to answer
Other
Don't know

Preventive measures

Eurobarometer 2008 (Towards a safer use of the Internet for children in the EU – a parents' perspective), actions taken to ensure children's online safety

When your child uses the Internet at home, what do you usually do? <Always, Very frequently, Not very frequently, Never, DK/NA>
Make sure you stay nearby when your child is online
Sit with your child when s/he goes online
Ask/talk to your child about what s/he is doing or did online
Check the computer later, to see which sites your child visited
Check the messages in your child's e-mail account/instant messaging service
Check whether your child has a profile on a social networking site/online community
When your child is online, are there things that s/he is not allowed to do?
No restrictions
Spend a lot of time online talk to people they don't know in real life
Use email
Use instant messaging tools
Use chat rooms
Create a profile in an online community
Access certain websites
Download/play music
Download/play films
Download/play games
Buy online
Give out personal information
Some parents are restricting activities, while others are allowing more activities to their children online. I will list activities, and please tell for each if you allow them or not
Spend a lot of time online
Talk to people they don't know in real life
Use email/ instant messaging tools
Use chat rooms
Create a profile in an online community
Access certain websites
Download/play music, films, games
Buy online
Give out personal information
Does the computer – that your child uses at home – have installed any of the following software?
Filtering software (blocking certain websites/activities)
Monitoring software (recording where they go/what they do online)
No, none of them

UK Children Go Online children survey, 2003-2005, children's questionnaire, rules

Are there any of these things which you are NOT allowed to do on the Internet?
Give out personal information
Use email
Use chat rooms
Use instant messaging
Play games
Download things
Buy anything
Fill out forms or quizzes
Don't Know
None of these
Other

Australia (ABS), Children's Participation in Cultural and Leisure Activities Survey, 2009, actions taken for Internet personal safety and security

Actions taken for personal safety and security in Internet use at home
Placing the computer in a public area of the house
Installing an Internet content filter
Supervising or monitoring child's use of the Internet
Educating child about safe and appropriate use of the Internet
Any other actions?
No action taken

Crimes against Children Research Center, Youth Internet Safety Survey, 2005 (YISS-2), parent's questionnaire, protective measures

Blocks SPAM e-mail?
Blocks pop-up ads?
Filters sexually explicit images or websites?
Blocks or controls your child's use of chat rooms, e-mail, newsgroups or instant messaging?
Monitors your child's online activities?
Limits the amount of time your child can spend online?
Blocks personal information from being posted or e-mailed?
Uses a browser or search engine just for kids?

ITU's Child Online Protection Initiative National Survey, 2009, preventive measures

Available advice or guidelines	
Agencies, or equivalents, that have published any advice or guidelines on the safe or appropriate use of the Internet by children and young people	Ministry of Education
	Ministry of Communications
	Ministry of Trade or Business Affairs
	The Telecoms Regulator
	Internet Service Providers or other providers
	Mobile phone network operators
	Law enforcement agencies
	NGOs or civil society organizations
	Ministry of Health or Social Services
Where the advice or guidance has been published	On TV or radio, or other public media
	On the Internet
	In printed form (*e.g.* booklets/leaflets/posters/brochures)
Areas covered by the advice or guidance	Exposure to harmful/inappropriate content
	Exposure to bullying or harassment
	Exposure to sexual predators
	Exposure to travelling sex offenders (sex tourism)
	Exposure to fraud or to age-inappropriate commercial activity
	Over-use of or "addiction" to the technology
	How to report concerns or incidents
	Exposure to other forms of harmful/inappropriate content
Available awareness and training programmes	Programmes/policies within schools/educational establishments/youth groups/other bodies
	Programmes for parents
	Programmes for teachers or others who work with children and young people
	Programmes provided by other agencies, outside of the schools or educational system
	Future planned programme/policy initiatives on Internet safety for children and young people
Legal Framework	Laws concerning the protection of children and young people that apply in the real world apply equally to similar behaviours or actions on the Internet
	The possession of child pornography/child abuse images is an offence
	The possession of child pornography/child abuse images is an offence if linked to intention to distribute
Law enforcement	Programmes exist for law enforcement agencies to help officers understand and deal with online safety issues facing children and young people
	Law enforcement officers are trained to retrieve and analyse digital data taken from computers and the Internet
	Forensic resources are sufficient to meet the volume of Internet-related crimes against children needing investigation
National Focal Point	There is a national focal point or agency with a specific responsibility for promoting safety on the Internet for children and young people

Co-operation with the Internet industry	There is a hotline or other specific mechanism for reporting suspected illegal content on the Internet
	There is a hotline or other specific mechanism for reporting suspected illegal behaviour found or taking place on the Internet
	Main players in the Internet industry co-operate with the government and other relevant agencies in promoting the safe and appropriate use of the Internet by children and young people

APEC Children Protection Project Survey of national governments, 2009, open-ended questions about policy responses

1. Current experiences regarding information considered harmful to children within economies. (What kinds of issues is each economy concerned with?)
2. Current methods to manage access to information considered harmful to children
Please describe status of technology development in your economy (filtering technology, detecting technology, mobile phone and other handheld device specific technology, etc.)
Does your economy have relevant laws and regulation?
Contents of voluntary efforts, such as self-regulation? Does your economy have any self-regulation?
Does your economy have policies to improve literacy or raise awareness regarding these issues? What is the current situation of best practices by government or private sector regarding safe online practices? If there are some policies and practices, please provide an overview.
Please describe domestic cooperation framework in your economy. (Example: public-private partnerships, inter-ministerial cooperation, cooperation among businesses, etc.)
Does your economy cooperate internationally on these issues? If there is some international cooperation regime, please describe the overview.

Bibliography

Alexa (2010), *Top sites* page, http://www.alexa.com/topsites, (accessed 26 February, 2010).

Antezeta Web Marketing (2010), "Reflections on search engine optimization, web analytics and web marketing", http://www.antezeta.com/blog/web-statistics-suppliers.

APEC (Asia-Pacific Economic Cooperation) (2009), "Answers to APEC Children Protection Project Questionnaire", 2009/TEL39/SPSG/SYM/018, http://www.oecd.org/document/17/0,3343,en_2649_34223_43301457_1_1_1_1,00.html.

ABS (Australian Bureau of Statistics) (2008a), *How Australians Use Their Time, 2006* (Cat. No. 4153.0), www.abs.gov.au/ausstats/abs@.nsf/mf/4153.0.

ABS (2008b), *Australian Standard Offence Classification (ASOC), 2008 (Second edition*) (Cat. No. 1234.0), www.abs.gov.au/ausstats/abs@.nsf/mf/1234.0.

ABS (2009a), *Household Use of Information Technology, Australia, 2008-09* (Cat. No. 8146.0), www.abs.gov.au/ausstats/abs@.nsf/mf/8146.0.

ABS (2009b), *Internet Activity, Australia, June 2009* (Cat. No. 8153.0), www.abs.gov.au/ausstats/abs@.nsf/mf/8153.0.

Canadian Centre for Child Protection (2009), *Child Sexual Abuse Images: An Analysis of Websites by cybertip!ca,* http://www.protectchildren.ca/app/en/media_release.

Census and Statistics Department, Hong Kong, China (2009), *Thematic Household Survey Report No. 43: Information Technology Usage and Penetration*, http://www.info.gov.hk/digital21/eng/statistics/it_survey2009.html.

CHI (Child Helpline International) (2010), "Violence Against Children: Fourth CHI VAC Questionnaire (draft)", unpublished.

CNNIC (China Internet Network Information Center) (2009), *Statistical Report on Internet Development in China: 24th Statistical Report on Internet Development in China*, http://www.cnnic.net.cn/en/index/0O/02/index.htm.

Cisco Systems Inc (2009), *Cisco Visual Networking Index: Forecast and Methodology, 2008–2013*, http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360.html.

comScore (2008), "Social Networking Explodes Worldwide as Sites Increase their Focus on Cultural Relevance", http://www.comscore.com/Press_Events/Press_Releases/2008/08/Social_Networking_World_Wide.

comScore (2009), "Twitter Traffic Explodes...And Not Being Driven by the Usual Suspects!", http://blog.comscore.com/2009/04/twitter_traffic_explodesand_no.html.

comScore (2010), *International solutions* page, http://www.comscore.com/International_Solutions (accessed 2 March 2010).

Cox Communications (in partnership with the NCMEC and John Walsh) (2007), *Cox Communications Teen Internet Safety Survey, Wave II*, http://www.cox.com/takeCharge/survey_results.asp.

EC (European Commission) (2004), *Eurobarometer. Illegal and harmful content on the Internet: EU-25 Comparative highlights,* http://ec.europa.eu/information_society/activities/sip/surveys/index_en.htm.

EC (2006), *Eurobarometer. Safer Internet,* http://ec.europa.eu/information_society/activities/sip/surveys/index_en.htm.

EC (2007), *Eurobarometer. Safer Internet for children: qualitative study in 29 European countries: summary report,* http://ec.europa.eu/information_society/activities/sip/surveys/index_en.htm.

EC (2008), *Eurobarometer. Towards a safer use of the Internet for children in the EU – a parents' perspective: summary,* http://ec.europa.eu/information_society/activities/sip/surveys/index_en.htm.

Eurostat (2009a), *Methodological Manual for Statistics on the Information Society,* years 2006-2009, http://circa.europa.eu/Public/irc/dsis/emisannexes/library?l=/data_-_database/theme_3_-_popul/isoc/methodological_informati&vm=detailed&sb=Title.

Eurostat (2009b), Model ICT use questionnaires, years 2002-2010, http://circa.europa.eu/Public/irc/dsis/emisannexes/library?l=/data_-_database/theme_3_-_popul/isoc/householdsindiv&vm=detailed&sb=Title.

Eurostat (2009c), *Information Society Statistics* homepage, http://epp.eurostat.ec.europa.eu/portal/page/portal/information_society/introduction.

Facebook (2010a), "Measurement Firms Don't Agree on January 2010 Traffic for Facebook, MySpace and Twitter", http://www.insidefacebook.com/2010/02/24/measurement-firms-dont-agree-on-january-2010-traffic-for-facebook-myspace-and-twitter/.

Facebook (2010b), *Company Timeline* page, http://www.facebook.com/press/info.php?timeline (accessed 1 August, 2010).

Facebook (2010c), *The Facebook Blog* page, http://blog.facebook.com/blog.php?post=409753352130 (accessed 1 August, 2010).

Facebook (2010d), *Statistics* page, http://www.facebook.com/press/info.php?statistics (accessed 1 August, 2010).

Facebook (2010e), "Facebook's February 2010 US Traffic by Age and Sex: All Groups Growing, Men More Quickly", http://www.insidefacebook.com/ (accessed 2 March, 2010).

Facebook (2010f), *Safety* page, http://www.facebook.com/help/?safety (accessed 7 March 2010).

Facebook (2010g), "Facebook Asks More Than 350 Million Users Around the World To Personalize Their Privacy", http://www.facebook.com/press/releases.php?p=133917.

Hasebrink, U., S. Livingstone, L. Haddon. and K. Ólafsson (2009), *Comparing children's online opportunities and risks across Europe: Cross-national comparisons for EU Kids Online*, http://www.lse.ac.uk/collections/EUKidsOnline/Reports/Default.htm.

IDA (Infocomm Development Authority of Singapore) (2009), *Annual Survey on Infocomm Usage in Households and by Individuals for 2008,* http://www.ida.gov.sg/Publications/20090218183328.aspx.

INHOPE (International Association of Internet Hotlines) (2007), *2007 Global Internet Trend Report*, https://www.inhope.org/en/node/296.

ITU (International Telecommunication Union) (2005), *WSIS Outcome Documents: Geneva 2003 – Tunis 2005,* http://www.itu.int/wsis/outcome/booklet.pdf.

ITU (2007), *Telecommunication/ICT Indicators Handbook*, http://www.itu.int/ITU-D/ict/handbook.html.

ITU (2008), *Use of Information and Communication Technology by the World's Children and Youth: a Statistical Compilation*, http://www.itu.int/ITU-D/ict/material/Youth_2008.pdf.

ITU (2009a), *Guidelines for Children on Child Online Protection*, http://www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/index.html.

ITU (2009b), *Guidelines for Parents, Guardians and Educators on Child Online Protection*, http://www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/index.html.

ITU (2009c), *Guidelines for Industry on Child Online Protection*, http://www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/index.html.

ITU (2009d), *Guidelines for Policy Makers on Child Online Protection*, http://www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/index.html.

ITU (2009e), *World Telecommunication/ICT Indicators Database 2009, 13th edition*, http://www.itu.int/ITU-D/ict/publications/world/world.html.

ITU (2009f), *Manual for Measuring ICT Access and Use by Households and Individuals,* http://www.itu.int/ITU-D/ict/publications/hhmanual/2009/index.html.

ITU (2009g), "Child Online Protection (COP) Initiative – National Survey 2009", http://www.itu.int/ITU-D/COP-survey.html (accessed 7 March 2010).

ITU (2010a), *Child Online Protection (COP) Initiative: National Survey 2009 Report*, http://www.itu.int/osg/csd/cybersecurity/gca/cop/Reports/DRAFT_COP_SurveyV5jcfinal_21July.pdf.

ITU (2010b), *Telecommunication/ICT Indicators Handbook*, http://www.itu.int/ITU-D/ict/handbook.html.

Internet Safety Technical Taskforce (2008), *Enhancing Child Safety and Online Technologies: Final Report of the Internet Safety Technical Taskforce*, http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report.pdf.

KISA (Korea Internet and Security Agency) (2009), *Survey on the Internet Usage*, *2009 11*, http://isis.kisa.or.kr/eng/board/?pageId=040100.

Livingstone, S. and M. Bober (2004), *UK Children Go Online: Surveying the experiences of young people and their parents*, http://www.lse.ac.uk/collections/children-go-online/.

Livingstone, S. and M. Bober (2005), *UK Children Go Online: Final report of key project findings,* www.lse.ac.uk/collections/children-go-online/.

Livingstone, S. and L. Haddon (2009a), *EU Kids Online: Final Evaluation Report*, EU Kids Online, http://www.lse.ac.uk/collections/EUKidsOnline/Reports/Default.htm.

Livingstone, S. and L. Haddon (2009b), *EU Kids Online: Final Report*, EU Kids Online, http://www.lse.ac.uk/collections/EUKidsOnline/Reports/Default.htm.

Lobe, B., S. Livingstone, K. Olafsson and J. Simões (Editors) (2008), *Best Practice Research Guide: How to research children and online technologies in comparative perspective*, EU Kids Online, http://www.lse.ac.uk/collections/EUKidsOnline/Reports/Default.htm.

MCIT (Ministry of Communications and Information Technology, Egypt) (2010), "Egypt's e-Safety Profile: One Step Further Towards a Safer Online Environment", presentation to the *Second Meeting of the Council Working Group on Child Online Protection (CWG-CP)*, Geneva, July, 2010.

Ministry of Internal Affairs and Communications, Japan (2008), "Communications News", Vol. 19, No. 10, http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/statistics.html.

MySpace (2010), *Safety* page, http://www.myspace.com/index.cfm?fuseaction=cms.viewpage&placement=safety_pageresources. (accessed 7 March 2010).

NIDA (National Internet Development Agency of Korea) (2009), *Survey on the SNS usage*, http://www.nida.or.kr/english/newsnnotice/news_view.jsp?gubun=1&menu=1&brdId=060315162942001000&aSeq=090730150644001001.

National Police Agency (2010), "The situation of child protection in Japan", http://www.npa.go.jp/english/index.htm.

National Statistical Office of Thailand (2007), "The 2007 ICT survey on household". http://web.nso.go.th/survey/ict/ict_house07.htm.

National Statistical Office of Thailand (2010), "Measuring household ICT access and individual use", presentation to *International Seminar on Information and Communication Technology Statistics*, Seoul, Republic of Korea, July, 2010, http://unstats.un.org/unsd/ict/.

The Nielsen Company (2009), *Global Faces and Networked Places*, http://blog.nielsen.com/nielsenwire/nielsen-news/social-networking-new-global-footprint/.

The Nielsen Company (2010), *Ratings and Rankings: Internet* page, http://en-us.nielsen.com/rankings/insights/rankings/internet (accessed 26 February, 2010).

ONS (Office for National Statistics) (2006), *The Time Use Survey, 2005, How we Spend our Time*, London, www.timeuse.org/information/publications/docs/TimeUse2005.pdf.

OECD (Organisation for Economic Co-operation and Development) (2005), *Guide to Measuring the Information Society, 2005*, www.oecd.org/sti/measuring-infoeconomy/guide.

OECD (2008), *Information Technology Outlook*, http://www.oecd.org/document/20/0,3343,en_2649_33757_41892820_1_1_1_1,00.html#HTO.

OECD (2009a), *Guide to Measuring the Information Society, 2009*, www.oecd.org/sti/measuring-infoeconomy/guide.

OECD (2009b), *Communications Outlook, 2009*, http://www.oecd.org/document/20/0,3343,en_2649_33757_41892820_1_1_1_1,00.html#HTO.

OECD (2010), "The Protection of Children Online", Preliminary Draft REV1, unpublished.

Partnership on Measuring ICT for Development (2005), *Core ICT Indicators*, http://www.itu.int/ITU-D/ict/partnership/material/CoreICTIndicators.pdf.

Partnership on Measuring ICT for Development (2007), "Report of the Partnership on Measuring Information and Communication Technologies for Development: information and communication technology statistics", Report to UN Statistical Commission, Thirty-eighth session, http://unstats.un.org/unsd/statcom/doc07/2007-5e-ICT.pdf.

Partnership on Measuring ICT for Development (2008), *The Global Information Society: a Statistical View, 2008,* http://www.unctad.org/en/docs//LCW190_en.pdf.

Partnership on Measuring ICT for Development (2010), *Core ICT Indicators*, http://www.itu.int/ITU-D/ict/partnership/material/Core%20ICT%20Indicators%202010.pdf.

Pew Internet and American Life Surveys (2007a), *Teens, Privacy and Online Social Networks,* http://www.pewinternet.org/.

Pew Internet and American Life Surveys (2007b), *Teens and Social Media,* http://www.pewinternet.org/.

Pew Internet and American Life Surveys (2009), *Teens and Sexting,* http://www.pewinternet.org/.

Pew Internet and American Life Surveys (2010), *Social Media & Mobile Internet Use Among Teens and Young Adults,* http://www.pewinternet.org/.

UNCTAD (United Nations Conference on Trade and Development) (2009), *Manual for the Production of Statistics on the Information Economy*, Revised Edition, Geneva, http://new.unctad.org/templates/Page____885.aspx.

UNESCO (United Nations Educational, Scientific and Cultural Organization) (1997), *International Standard Classification of Education*, http://www.uis.unesco.org/ev.php?ID=3813_201&ID2=DO_TOPIC.

UIS (UNESCO Institute for Statistics) (2009), *Guide to Measuring Information and Communication Technologies (ICT) in Education*, http://www.uis.unesco.org/template/pdf/cscl/ICT/ICT_Guide_EN.pdf.

United Nations General Assembly (1989), *Convention on the Rights of the Child*, 20 November 1989, United Nations, Treaty Series, vol. 1577, p. 3, http://www.unhcr.org/refworld/docid/3ae6b38f0.html.

UNSC (United Nations Statistical Commission) (2007), "Report on the thirty-eighth session (27 February to 2 March 2007)", E/2007/24 and E/CN.3/2007/30, New York, http://unstats.un.org/unsd/statcom/doc07/FinalReport-Unedited.pdf.

UNSC (2009), "Report on the fortieth session (24 to 27 February 2009)", E/CN.3/2009/29, New York, http://unstats.un.org/unsd/statcom/doc09/Report-English.pdf.

UNSD (United Nations Statistics Division) (2008a), *Principles and Recommendations for Population and Housing Censuses Revision 2,* http://unstats.un.org/unsd/demographic/standmeth/principles/Series_M67Rev2en.pdf.

UNSD (2008b), *International Standard Industrial Classification of All Economic Activities (ISIC), Rev. 4*, http://unstats.un.org/unsd/cr/registry/isic-4.asp.

UNSD (2010), *Standard country or area codes for statistical use,* http://unstats.un.org/unsd/methods/m49/m49.htm.

WAA (Web Analytics Association) (2008), *Web Analytics Definitions*, http://www.webanalyticsassociation.org/?page=standards.

Wolak, J., K. Mitchell and D. Finkelhor (2006), *Online victimization of youth: five years later*, http://www.unh.edu/ccrc/internet-crimes/papers.html.

Wolak, J., D. Finkelhor and K. Mitchell (2009), *Trends in arrests of "online predators"*, http://www.unh.edu/ccrc/national_juvenile_online_victimization_publications.html.

World Congress III against Sexual Exploitation of Children and Adolescents (2008), "Adolescent Declaration to End Sexual Exploitation", Annex to *The Rio de Janeiro Declaration and Call for Action to Prevent and Stop Sexual Exploitation of Children and Adolescents*, http://www.ecpat.net/WorldCongressIII/PDF/Outcome/WCIII_Outcome_Document_Final.pdf.

Geneva, October 2010