Harvard Law School
Public Law & Legal Theory Working Paper Series
Paper No. 10-36

Working Towards a Deeper Understanding of Digital Safety for Children and Young People in Developing Nations

Urs Gasser
Harvard Law School

Colin M. Maclay

John G. Palfrey Jr.
Harvard Law School

Working Towards a Deeper Understanding of Digital Safety for Children and Young People in Developing Nations

An Exploratory Study by the Berkman Center for Internet & Society at Harvard University, in Collaboration with UNICEF

June 16, 2010

Authors:
Urs Gasser, Colin Maclay, John Palfrey

Berkman Center Research Assistants:
Sandra Cortesi, Lauren Dyson, Rachel Miller-Ziegler

Collaborators at UNICEF:
Gerrit Beger, Katherine Maher, Merrick Schaefer

Comments welcome at ugasser [at] cyber.law.harvard.edu

1 Introduction

1.1 Background

Youth & Media Debates

[1] The growing importance of digital technologies in general and the Internet in particular in the lives of today's young people has stimulated a lively debate about both the benefits and challenges of the use of information and communication technologies.[1] The discussion covers an exceedingly broad range of issues, including perceived opportunities such as online learning and new forms of civic engagement, as well as risks, such as Internet addiction and privacy concerns. Promise, problems, and the unknown are intermingled and of increasingly widespread interest, although the debate is not well informed by experience. Despite that appeal, this modest paper will not explore them all.

Children's Safety Online

[2] These issues are not only discussed among parents and teachers, but have also reached the agendas of researchers, policy-makers, and the public at large. Perhaps not surprisingly, much public attention – often triggered by extensive media coverage of tragic stories involving young people and digital media – has been paid to the concerns related to the safety of children and young people.[2] Beyond these important but anecdotal events, digital safety has become an important research topic, leading to an already significant and further growing body of scholarly contributions. Arguably, this scholarship is increasingly oriented toward and based upon quantitative research and, at least in some areas, has reached a degree of maturity where policy recommendations and action plans can be based upon it.[3]

Knowledge gaps

[3] Despite the progress that has been made in gaining a deeper understanding of child digital safety issues, and actions that can be taken to address some of the underlying challenges, several

[1] See, e.g., Palfrey & Gasser (2008)

[2] We use the term "children" in accordance with The United Nations Convention on the Rights of the Child for human beings under the age of 18 years. The term "young people" is broader and includes young adults (as well as children).

[3] See, e.g., Internet Safety Technical Task Force, Enhancing Child Safety and Online Technologies: Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States; Safer Children in a Digital World The Report of the Byron Review, March 2008.

important research questions in this quicksilver technological environment remain open and deserve further research. Probably the most glaring gap in the research landscape, however, is less topical and more geographical or socio-economic in nature: Most of the relevant research (with a small number of important exceptions) has focused on safety implications of Internet usage of young people in industrialized nations, usually with emphasis on Western Europe and Northern America. Despite recent efforts (in the context of the Internet Governance Forum, for instance), much less is known about digital safety risks to children in developing and emerging economies.[4] This knowledge gap is particularly relevant in a time where the difference in access to Internet and communication technologies between industrialized and developing nations is arguably narrowing.[5] The digital world brings many new opportunities and resources into the lives of young people in developing nations, but it also exposes new groups – typically with lower levels of digital literacy – to a range of new threats. These threats are exacerbated by other common weaknesses in developing nation settings, including limited institutional capacity, financial resources, and other means of mitigating and addressing these threats and problems, especially in the face of other pressing concerns. With leaders striving to address these challenges and scant information upon which to base their responses, they may be forced to choose between suboptimal policy and legal actions, or inaction.

1.2 Objectives

Overview

[4] This exploratory study is a first output of an ongoing collaboration between the Berkman Center for Internet & Society at Harvard University and UNICEF. It is intended as a contribution towards building a deeper understanding of children's safety in a digital context in developing nations. More specifically, the objectives

[4] In this paper, we use the term "developing nations" for all low- and middle-income countries, acknowledging important differences in development among these economies. In accordance with international practice, the designations "industrialized" and "developing" are used for statistical convenience and do not express a judgment about the stage reached by a particular country or area in the development process, see e.g., http://unstats.un.org/unsd/methods/m49/m49.htm.

[5] See, e.g. IGF 2008 Workshop 36 report: "Strategies to prevent and fight child pornography on Developing Countries", available at http://www.intgovforum.org/cms/index.php/2008-igf-hyderabad/event-reports/72-workshops/353-workshop-36-strategies-to-prevent-and-fight-child-pornography-on-developing-countries.

of the paper are threefold: First (and foremost), it seeks to raise awareness about issues related to digital safety for youth in developing nations. Second, it aims to provide a tentative map of these issues and give insights into the current state of the respective research based on an exploratory literature review. Third, the paper seeks to outline the contours of a research framework through a series of working hypotheses that might inform subsequent research efforts on these issues by connecting efforts in developing and industrialized nations.

Approach

[5] The topic of this paper is challenging along a number of dimensions, including the complexity of the subject of investigation, cultural expectations and tolerance, language barriers, the highly limited availability of data, and limited access to scholarship from developing nations to the extent that it exists. We therefore decided not only to take a collaborative approach to research this paper (see methodology paragraph below), but also to release it as a "learning document" by soliciting feedback, comments, pointers to additional materials, etc. At the end of such a participatory period and after additional research on our end, the hope is to publish a revised and extended version of this paper in the format of a white paper.

1.3 Methodology

Overview

[6] We have combined a number of methodologies in the research process leading up to this paper. Our efforts include, among other things, extensive Web and database searches, a review of anecdotal evidence, the drafting of case studies, an exploratory literature review, various expert interviews, and a survey among experts on technology, learning, and child safety in the developing world. More specifically:

Web-Search

[7] Researchers at the Berkman Center began with a comprehensive Web search (in English) of organizations and initiatives that are working to make information and communication technologies available to children in developing nations to improve education and quality of life. An in-progress list of the organizations can be found on the project's wiki.[6]

[6] See http://www.digitalnative.org/wiki/Child_online_safety_in_the_developing_world#How_you_can_contribute#Organizations

[8] Based on this exploratory Web search and conversations with online safety experts in both the developing and developed worlds, we drafted a questionnaire aimed at gathering information about the existing research and work that has been done in the area of digital safety for children and young people in developing nations. This questionnaire was sent in personalized e-mails to dozens of individuals (researchers, practitioners, activists, social workers, etc.) and organizations (including non-governmental, international, academic and private sector) based on a list initially created in collaboration with UNICEF, and expanded as a snowball sample based on participant feedback. The responses have been briefly summarized on the project's wiki.[7] Parts of the questionnaire were also sent to local UNICEF representatives in more than 150 countries. *Survey*

[9] Based on the results of these searches and the input we received from child safety experts, we conducted a preliminary literature review on child online safety issues in the developing world. We have focused primarily on English language sources, but have actively solicited inputs on non-English language materials as well. Given the scope and objectives of this paper, it should be noted that the literature review is exploratory in nature and only serves as a starting place for a more comprehensive, multilingual review of a possible follow-up research project on this particular topic.[8] *Literature review*

2 Contextualizing Digital Safety for Children and Young People

2.1 Overview

[10] Digital safety for children and young people is not a coherently framed, clear-cut concept. Rather, it is a vague term that refers to a diverse set of issues that are directly or indirectly related to the physical and psychological well-being of children who use digital media, focusing not on a particular access technology, such as an *Risk and context*

[7] See http://www.digitalnative.org/wiki/Community_contributions.

[8] Despite our concerted efforts to identify relevant literature, our inquiry has only resulted in a small number of studies, reports, and/or academic contributions. The impression that child online safety in the developing world context is an under-researched topic was confirmed by various responses to our questionnaire, where we also asked about foreign-language studies and reports. Consequently, we have not limited our review to particular subset of developing countries.

Internet connection, mobile phone or some other means, but on the broader characteristics of digital media. It is difficult to come up with a comprehensive, yet sufficiently specific definition of "safety", and it seems more productive to identify risks that might threaten a broadly understood concept of digital safety.[9] Several years of research on this topic leave little doubt that the respective digital risks are highly contextual in at least two respects. On one hand, risks (as well as the opportunities) of digital media for children depend on what we might call micro-level factors, including setting and means of access, usage patterns, attitudes and skill levels. Age, gender, socio-economic status as well as peer behavior and mediation by caregivers are other factors to be considered at the level of the individual child. On the other hand, several of these child-centric factors are influenced by a set of interacting macro-level parameters, ranging from big-picture economic to cultural and societal characteristics. This section of the paper focuses on such contextual factors at the national or regional level.

Framework

[11] The following framework developed by the EU Kids Online Project[10] summarizes some of the key factors that explain cross-national differences when it comes to children's access to, use of, and risks with digital media. While the framework has been developed to explain differences across Europe, and is specific to the use of the Internet by children and young people, it seems also helpful in the developing world context of this paper by at least illustrating the broad range of issues that need to be taken into account as contextual factors likely to shape risks and, in turn, safety of children and young people in digital spaces.

[9] Byron Review, p. 16.
[10] Sonia Livingstone and Leslie Haddon, EU Kids Online: Final Report, p. 20 et seq.

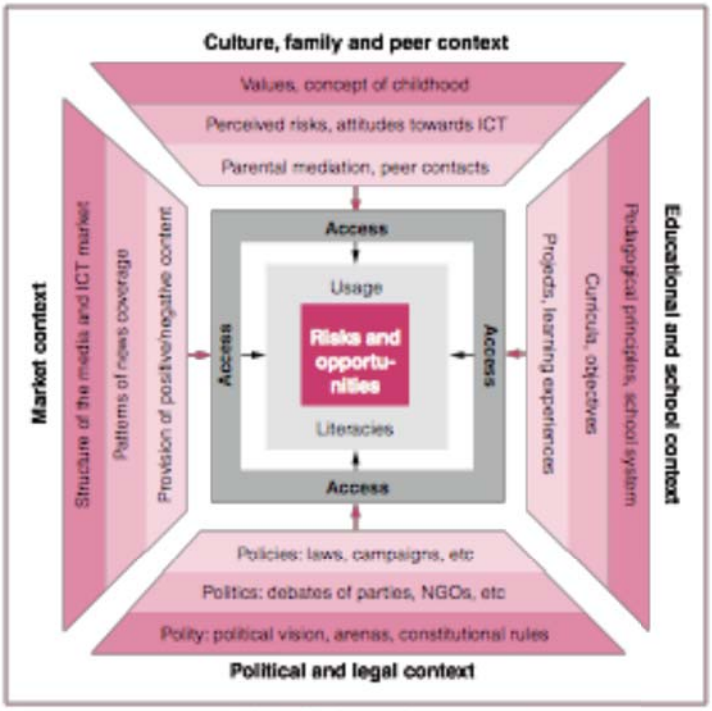

Figure 13: Contextualising children's internet use

[12] A detailed analysis of all the factors identified in the framework (several others could be added) is beyond the purpose and scope of this paper. Moreover, the lack of sufficient comparable data from developing nations makes it nearly impossible to provide such a comprehensive analysis. In the following paragraphs, we therefore roughly cluster the various factors among three dimensions (technological, economic and market context – educational and cultural context – legal and political context) and provide a very brief overview of the ways in which each cluster may interact with child-centric factors such as access, usage, and skills, among others (along the lines of the micro-level factors introduced earlier). This overview is then illustrated by a small numbers of examples from the developing world. The examples are primarily of illustrative purpose, but may also serve as anecdotal evidence and inspire future research efforts in the field.

Limitations

2.2 Selected Safety-Relevant Contextual Factors

2.2.1 Technological, Economic, and Market Context

Overview

[13] Risks and opportunities of digital connectivity are shaped by a variety of characteristics at the individual level that include access to and usage of digital technologies, described earlier as micro-factors. These factors are, in turn, influenced by the broader social, economic and technological conditions in which an individual lives and, in particular, under which the Internet can be accessed, discussed as macro-factors. It is well established, for example, that socio-economic status plays a decisive role with regard to access to and use of the Internet in countries where access has not become commonplace. Focusing on ICT infrastructure, a look at recent statistics reveals massive differences among continents, regions and countries when it comes to Internet diffusion in general and broadband penetration in particular.[11] Although the price for fixed broadband access remains prohibitively high in many developing nations, studies indicate that at least some nations – such as India and China – are gaining on OECD countries in terms of Internet usage and broadband penetration. While the least developed nations may be left behind in terms of fixed connectivity (for now), they are catching up on mobile connectivity.[12] The following examples seek to illustrate some of these broader contextual themes.

Example: Access technologies

[14] Perhaps the most visible distinction between developed and developing nations is the means of digital communication for children and young people. Mobile phones have fast become fundamental tools in the developing world – especially in the least developed countries, in contrast to industrialized nations, where IP-based Internet is the dominant digital tool. In fact, most of the growth in the mobile phone market is in developing nations, especially in Africa and Asia.[13] As discussed below, the widespread use of mobile phone has safety implications, for instance by facilitating new forms of sexual exploitation of children, or by limiting parental control over communications.

Example: Access location

[15] Also, statistics show important differences between the developing and industrialized nations with regard to linkages among

[11] See, e.g., The World in 2009: ICT Facts and Figures, ITU-D (2009)
[12] See, e.g., ITU/UNCTAD 2007 World Information Society Report: Beyond WSIS, 2007, p. 8.
[13] See, e.g., ITU/UNCTAD 2007 World Information Society Report: Beyond WSIS, 2007.

socio-economic micro-factors (income in particular) and locations of access. For users in the West and more developed Asian economies, home is the most likely location of Internet use, whereas it is less common as a place of use in developing economies, reflecting lower levels of household Internet access. Current data, however, does not provide a clear picture regarding preferred access location in the developing world. For some countries, including Brazil and Thailand, the data shows higher rates of use for commercial access facilities, while the situation might be different in other developing nations where users may be more reliant on public or subsidized access, such as schools and community centers.[14]

Example: Market players

[16] Depending on the specific context, important differences exist with regard to market players who are providing access to the Internet in general and co-facilitate safety-relevant behavior in particular. Several reports from the developing world, for instance, have highlighted the role of Internet cafés, but not only in terms of accessing harmful materials. According to an ongoing case study by UNICEF Philippines, for instance, children and adults alike are reported to be using Internet cafés to engage in sexually explicit conduct in public – a trend that has led to a multi-stakeholder initiative aimed at establishing child-friendly Internet cafés in the region.[15] (It should be noted, however, that the problem in some countries is an inverse one in the sense that users in Internet cafés are subject to extensive surveillance to ensure compliance with local rules and customs.[16])

2.2.2 Educational and Cultural Context

Overview

[17] A second important cluster of contextual macro-level factors that shape access, usage, attitudes and skills of young users can be subsumed under the broad categories "education" and "culture".

[14] See ITU, Use of Information and Communication Technology by the World's Children and Youth, 2008, p. 19 et seq.

[15] UNICEF, The Role of the Private Sector, Particularly ISPs and Interne Café Owners, as Active Partners in Protecting Children from Sexual Abuse and Exploitation in the Philippines, An on-going Case Study by UNICEF Philippines (presentation, on file with authors). See also Bart Barendregt, Sex, phones and youth culture: Pornoaksi and the fear of new media in present day Indonesia, Asia Culture Forum 2006 (manuscript on file with authors).

[16] See, e.g., a report from China: http://www.ifex.org/china/2008/10/27/government_imposes_new_surveillance/

Various studies have examined the relationship between education and children's Internet usage. A leading European study, for instance, explains cross-national differences in children's online use in part by varying levels of general education, with higher levels of education leading to higher usage rates. A broad range of cultural factors also shapes the landscape of children's safety online. Soft factors range from general values (e.g. regarding sexuality, morality[17]) and conceptions of childhood that affect the ways in which adults mediate children's use of digital technologies, to peer culture and socially accepted expressions of friendship, to name just a few. Again, the following data points and examples only highlight a very small subset of factors that are often mentioned in the developing world literature to illustrate how context matters.

Example: Use of ICT in education

[18] Internet penetration in schools and the actual use of online technologies in educational settings have an impact on young user's online skills, but vary greatly among countries. Although there is currently limited data available on the use of ICT in education, it is safe to conclude that there are massive differences not only between industrialized and developing world, but also among and within developing nations. Recent data on schools with an Internet connection, but also statistics on basic infrastructure such as electricity, radio or telephone, are indicators about both the depth and breadth of the existing participation gaps among developing nations with regard to availability (and use) of the Internet in education.[18]

Example: Gender as cultural category

[19] An important cultural factor to take into account when it comes to Internet usage is socially rooted gender differences. Global statistics show similar rates of Internet use for boys and girls aged 5-14 as well as for the age group 15-24, with more exceptions (including Azerbaijan, Cyprus, and Occupied Palestinian Territory) in the latter category.[19] However, anecdotal evidence suggests that gender disparities may be highly relevant in at least some developing

[17] Illustrative in this context Linda A. Jackson, Yong Zhao, et al., Morality in Cyberspace: A comparison of Chinese and U.S. youth's beliefs about acceptable online behavior, Proceedings of the 41st Hawaii International Conference on System Science 2008, available at http://www.computer.org/portal/web/csdl/doi/10.1109/HICSS.2008.324

[18] See Partnership ON, The Global Information Society: a Statistical View, 2008, pp. 84-86.

[19] See ITU, Use of Information and Communication Technology by the World's Children and Youth, 2008, p. 23.

nations.[20] A report from Nigeria, for instance, draws our attention to gender relations when it comes to access and use of ICT and technology education for African girl-children. The report identifies "structural and cultural barriers in schools from home that contribute greatly to gender disparity in education generally, and in technology education in particular." This participation gap is partially illustrated by one study cited in the report, according to which girls were less than 20% of the total users of computers recorded in two cyber cafés in a given town, and that most of the girls present were sitting alongside boys who were operating the computers.[21] Naturally, understanding true gender differences in technology use goes much further, as does the need to understand the impact of technology use on gender.

2.2.3 Legal and Policy Context

Overview

[20] Policy and legal factors have many-faceted and often not easily measurable influences on access conditions, usage patterns, Internet attitudes and ICT skill levels in a given society. A cross-national study of children online in Europe, for instance, revealed a number of patterns that might at least serve as initial hypotheses for the developing world context. The study stipulates, for instance, a relationship between Internet diffusion and risk awareness by observing that in countries where the Internet is more common, risk awareness and (as a result) literacy initiatives seem to gain priority on the policy agenda.[22] Different legal traditions, approaches, techniques (e.g. direct regulation vs. self- or co-regulation), and law enforcement practices are also contextual factors that shape the safety landscape. In the European context, countries that are considered to be taking a liberal, i.e. less interventionist approach, appear to be higher risk environments for children online, according to a recent study.[23] The following examples further illustrate how some of the factors in this category may play out in the developing world context.

---

[20] See, e.g., Claudia Mitchell and Grace Sokoya, New Girl (and New Boy) at the Internet Cafe: Digital Divides/Digital Futures, in: Sandra Weber and Shanly Dixon, Growing Up Online: Young People and Digital Technologies, Palgrave: 2007, p. 214 et seq.

[21] See Josephine Nkiru Alumanah, Access and Use of Information and Communication Technology for the African Girl-child Under Cultural Impediments, Woman and ICT, June 12/15, 2005 [without pagination]

[22] See Sonia Livingstone and Leslie Haddon, EU Kids Online: Final Report, p. 21.

[23] Sonia Livingstone and Leslie Haddon, EU Kids Online: Final Report, p. 21.

[21] The importance of awareness-building as part of a public policy agenda is described in an exemplary way in a regional report on child sexual abuse images in Belarus, Moldova, Russia, and the Ukraine. The study summarizes it as follows: "The countries studied are facing a rapid increase in information and communication technologies supported by governmental policies that are actively pushing for the widespread development of the Internet nationally and especially in educational realms. As a result, an increasing number of children are accessing the Internet, creating new opportunities for learning and sharing information or socializing throughout the world. However, this has also led to an increasing number of cases of sexual exploitation, particularly as prevention and protection measures are not systematically included in the countries studied at the early stages of ICT development."[24]

Example: ICT policies

[22] An even more visible difference among developing (and to a lesser extent, also industrialized) nations is the legal treatment of the production, dissemination, storage and use of materials involving sexual abuse of children. According to a recent report, only 29 out of 187 Interpol member countries have legislation sufficient to combat child pornography offenses, and 93 countries have no legislation at all that specifically addresses child pornography.[25] The nationally and regionally varying definitions of what constitutes child pornography are another prominent example.[26] But not only might the definition of child pornography vary within a region, but also the definition of who is protected as a child under the law. Many more differences of this type could be added, for instance with regard to reporting obligations or liability of online intermediaries involved in the distribution of such materials.

Example: Child pornography laws

[24] ECPAT International, Regional Overview on Child Sexual Abuse Images through the Use of Information and Communication Technologies in Belarus, Moldova, Russia and Ukraine, September 2008, p. 8.

[25] See, e.g., International Centre for Missing & Exploited Children, Child Pornography: Model Legislation & Global Review, 2008.

[26] Deborah Muir, Violence Against Children in Cyberspace, A contribution to the United Nations Study on Violence against Children, ECPAT International, 2005, p. 42 et seq.

2.3 Working Hypotheses

2.3.1 General Observations

[23] The previous paragraphs put safety for children and young people in the digitally networked environment in context along at least three distinct dimensions:

Analytical perspective

[24] At the analytical level, the brief discussion of some of the relevant macro-level parameters illustrates the complexity of the ecosystem that needs to be taken into account when addressing child online safety in the developing world. The overview also amplifies the need for reliable data and the standardization of indicators across a broad spectrum of issues related to information and communication technologies (ICT) and illustrates the challenge of cross-country comparisons in light of the number of variables.

Policy perspective

[25] From a public policy angle, the online safety of young users is only one among many and often even more fundamental challenges faced by developing nations. Looking at recent trends that indicate a narrowing of the access gap through mobile technology, the overview also suggests the growing relevance of online safety as a policy issue, which requires monitoring and more research.

Normative perspective

[26] A normative perspective highlights the importance of pragmatic approaches when dealing with child online safety risks in the developing world. The significant conceptual and analytical challenges caused by the enormous complexity and lack of data and the unsatisfactory state of developing country-specific research in this field should not dispense with prompt action in areas where we already have at least some data, and in which context-sensitive interventions with in-built learning mechanisms can make a difference.

2.3.2 Specific Observations

[27] The high-level overview of the broad range of contextual macro-level factors that shape the child online safety landscape in the developing world suggests a number of specific observations, which may at least serve as starting points for hypotheses in the context of future, more in-depth research projects. These observations can be divided into contextual factors that are likely to have rather direct effects on the types of safety risks young users face, and

characteristics that are expected to have a significant impact on the development of tools in response to such challenges.

2.3.2.1 Risk Scenarios

Mobile phones

[28] Particularly noteworthy is the availability of relatively robust data that demonstrates the importance, indeed, primacy, of mobile phones as access devices in the youth context, especially in comparison with the industrialized world. Different access technology is very likely to have an impact on the character and quantity of child online safety issues and the particular characteristics of risk scenarios. The *potential* mediating effect of parents, teachers and other caregivers on Internet access and usage of their children, for instance, is different in the case of mobile phones when compared with laptops or PCs. Mobile phones enable young users to communicate with less adult supervision. Also, mobile phones foster particular types of communication when compared with other access devices. Text messaging, the ability to take and send images and videos, Global Positioning System (GPS) location applications, or the ability to follow-up immediately via live conversation are likely to be safety-relevant features of mobile phone technology, to name just a few.

Skills

[29] Research shows a connection between overall levels of education, media literacy and the use of online media. Recent studies have revealed significant differences in media competency across Europe and in the U.S., which have both an impact on the opportunities associated with Internet usage, and on its risks. The ICT statistics from developing nations referenced above illustrate a dramatic gap when it comes to access of education for children. This suggests even greater participation gaps and the creation of new types of inequalities with direct ramifications for risk exposure of children in the increasingly digital environment.

2.3.2.2 Safety Strategies

Education

[30] In the industrialized world, several strategies and instruments have been proposed in response to the safety risks that children encounter in digital spaces. Among the most promising approaches are educational strategies. The contextual overview of micro- and macro-level factors provided in the previous section should certainly not preclude educational approaches aimed at enhancing child digital safety as elements in the strategy mix of developing nations. The

brief remarks simply suggest that the location and approach to learning and the forms of education might be different in the developing world context. The relatively low degree of ICT usage in schools in many countries combined with the popularity of mobile phones and Internet cafés among young users suggest that the creation of learning opportunities outside of the classroom and education facilitated by peers are likely to be among the key elements of any promising strategy.

Regulatory Interventions

[31] Another response pattern in the digital safety area in industrialized nations are regulatory interventions, ranging from direct command-and-control legislation to more sophisticated model of co-regulation, where industry and governments play in concert in order to address some of the hardest-to-resolve safety issues. While specific legal and regulatory interventions might also be suitable in the developing nation context (the enactment of anti-child porn legislation is an example), the promise of such approaches should not be overestimated in nations where the rule of law has not been fully developed or in environments where basic elements of the legal infrastructure (such as efficient enforcement regimes) might turn out to be nascent.

3 Identifying Child Digital Safety Issues

3.1 Overview

Approach

[32] The previous section emphasizes the contextual nature of digital safety, which suggests that related risks need to be identified, analyzed, and evaluated based on a country-specific (perhaps even sub-national), data-driven bottom-up approach. Such an approach has many advantages; it draws our attention to actual rather than merely theoretical risks, allows us to add new risk categories as they emerge (take, for instance, "sexting" as such a recent development), and ensures tailored response strategies. One disadvantage, however, is that such an approach makes the identification of digital risks very difficult when moving into environments where we lack data and where the primary focus is on qualitative horizon scanning, emerging issues analysis, and risk assessment.

Tentative framework

[33] While we acknowledge the need for and benefits of data-driven approaches aimed at identifying and rationalizing digital safety risks for children and young people, we propose for the context and

purpose of this paper the use of a tentative framework that seeks to structure the main set of factors that constitute digital safety risks and aims to map the various possible risk clusters. The following matrix developed by the EU Kids Online Project is helpful to at least *tentatively* identify and cluster the various online risks faced by young people and children in the context of developing nations:[27]

	Commercial	Aggressive	Sexual	Values
Content (child as recipient)	Adverts Spam Sponsorship Personal info	Violent/hateful content	Pornographic or unwelcome sexual content	Bias Racist Misleading info or advice
Contact (child as participant)	Tracking Harvesting personal info	Being bullied, harassed or stalked	Meeting strangers Being groomed	Self-harm Unwelcome persuasions
Conduct (child as actor)	Illegal downloading Hacking Gambling Financial scams Terrorism	Bullying or harassing another	Creating and uploading inappropriate material	Providing misleading info/ advice

[34] Based on that framework, we have identified a series of research outputs across developing nations that provide anecdotal clues and, in rare instances, empirical evidence of specific digital safety risks for children and young people. The reviewed materials vary greatly in approach, scope, depth, and tone, and we have not been able to find materials for all possible risk clusters of the framework. Following a pragmatic approach, the following subsection acknowledges that there is a lot that we do not know, but tries to work towards a deeper understanding based upon the relatively little information that we have so far.

[27] The evaluation of the identified risks, however, will very much depend on contextual factors.

3.2 Selected Risk Clusters

3.2.1 New Forms of Production of Child Abuse Images

Phenomenon

[35] Digital technologies have dramatically changed the ways in which images of sexual abuse and exploitation of children can be produced and distributed. A thorough discussion of this multi-faceted and complex social phenomenon and its effects on children in developing nations is outside the scope of this paper. However, the trend towards real-time creation of pornography—which may include child pornography, depending on the definition—by using Web cams and other online technologies has been flagged in the reviewed literature as an emerging issue, particularly (but not only) in the developing nation context.[28]

Anecdotal Evidence

[36] A scholarly article on sex and technology-enabled youth culture issues in Indonesia discusses new forms of production and distribution of pornographic materials by highlighting the role of Internet cafés in a country where broadband Internet connections to the home is still low. While users of cyber cafés might be monitored once they open suspicious Websites, many of these cafés reportedly have private booths equipped with PC and Web cam, which are used by girls for online striptease shows in return for money transferred to their pre-paid mobile phone accounts.[29] Similar problems are reported from the Philippines, where profit-making ventures have emerged that feature adolescents performing sexual acts in front of Web cameras, following instructions of users who pay by credit card.[30]

3.2.2 Sexting

Phenomenon

[37] Sexting (a portmanteau of sex and texting) refers to a relatively recent social practice among teenagers and young adults who send sexually explicit messages, photos, or video clips over mobile phones.

---

[28] See Marie-Laure Lemineur Retana: El Combate Contra La Pornografia Infantil en Internet: El caso de Costa Rica, International Labor Organization/International Program for the Eradication of Child Labor 2006.

[29] Bart Barendregt, Sex, phones and youth culture: Pornoaksi and the fear of new media in present day Indonesia, Asia Culture Forum 2006, p. 5 (manuscript on file with authors).

[30] See Arnie C. Trinidad, Child Pornography in the Philippines, Psychosocial Trauma and Human Rights Program UP Center for Integrative and Development Studies and UNICEF Manila 2005.

While more research is needed, recent surveys from the industrialized world indicate that sexting is a phenomenon of increasing relevance in the context of digital safety for children and young people, which links the production and dissemination of child porn (see previous paragraph) with the issues of exposure to pornography and harassment (see subsequent paragraphs).[31] The exploratory literature review has not revealed reliable data on this phenomenon in the developing nation context. However, sexting has been mentioned in a number of academic papers.

Anecdotal Evidence

[38] A report from Indonesia, for example, demonstrates how mobile phone cameras are used by teenagers to produce clips featuring girls and boys engaged in sexually explicit behavior, and highlights the role of mobile phones in the distribution and access of harmful materials—a phenomenon that has led to police inspections of individual mobile phones in several Indonesian schools.[32] A study of adolescent girls' use of mobile phones in Cape Town discusses, among other things, the practice of sexual experimentation over MXit, a popular South African based instant messaging application that runs on GPRS/3G mobile phones with Java support. Interviews with young users confirm exposure to undesirable images in peer relationships and indicate differences in how photographs were used by girls and boys.[33] Reports from India also confirm that sexting is an emerging phenomenon.[34]

3.2.3 Exposure to Pornography

Phenomenon

[39] Digital technologies have not only affected the ways in which harmful, problematic and illegal content is produced, but has also made it easier for users to access such materials.[35] A comprehensive review of existing research in the U.S. recently confirmed the increased availability of harmful materials, but concluded that the

[31] According to a 2009 Pew Internet survey, 8% of 17 year-olds with mobile phones had sent a sexually provocative image by text, and 30% had received a nude or nearly nude image on their phone, online at http://www.pewinternet.org/Reports/2009/Teens-and-Sexting.aspx

[32] Bart Barendregt, Sex, phones and youth culture: Pornoaksi and the fear of new media in present day Indonesia, Asia Culture Forum 2006, p. 13 (manuscript on file with authors).

[33] Tanja E. Bosch, Wots ur ASLR? Adolescent girls' use of cellphones in Cape Town, April 25, 2008, p. 6 and p. 17 (manuscript on file with authors)

[34] See Lina Acca Mathew, Online Child Safety from Sexual Abuse in India, 2009(1), Journal of Information, Law & Technology (JILT), at http://go.warwick.ac.uk/jilt/2009_1/mathew.

[35] See, e.g., Deborah Muir, Violence Against Children in Cyberspace, A contribution to the United Nations Study on Violence against Children, ECPAT International, 2005, pp. 52-58.

Internet does not always lead to increased exposure of children.[36] Western research shows that unwanted exposure to pornography does occur online, but also points out that those most likely to be exposed are those seeking it out. Research from other parts of the world (e.g. from the Republic of Korea), suggests a rising number of complaints about online pornography and unwanted youth exposure.[37] Children's exposure to pornography has also been identified as an issue in the developing context.

Anecdotal Evidence

[40] Data from a survey in Thailand, for instance, suggests that 35% of seven- to eleven-year-olds have had exposure to Websites displaying pornographic content.[38] Among older respondents, 71% have voluntarily visited porn sites at least once. A report from the Philippines links increased access to pornographic sites by Filipino children to the proliferation of cyber cafés in urban areas: "If one visits these cyber cafés, it is no longer surprising to find children and teenagers who surf pornographic sites, with few cyber café operators stopping these children from accessing those pages."[39] Similar statements by researchers can be found, for instance, with regard to Internet cafés in Senegal, especially in Dakar.[40] A Chinese survey examining the relationship of Internet use and HIV knowledge of college kids and exploring the relationship between online risk behaviors and sexual status, sexual intention, and sexual perceptions finds that male students reported much higher rates of visiting pornographic Websites or engaging in other online risk behaviors. Students who "were sexually active, planned to have sex, or possessed permissive attitudes toward pre-marital sex were more likely to report online risk behaviors such as visiting pornographic sites, cyberbullying, or distributing erotic materials via the Internet."[41]

---

[36] ISTT report, p. 5.

[37] See Deborah Muir, Violence Against Children in Cyberspace, A contribution to the United Nations Study on Violence against Children, ECPAT International, 2005, p. 55 (with reference).

[38] Isabelle Michelet, Our Children at Risk Online: The Example of Thailand, in: A Survey Report, Our Children at Risk Online, The Example of Thailand, ECPAT International 2003, p. 15.

[39] See Arnie C. Trinidad, Child Pornography in the Philippines, Psychosocial Trauma and Human Rights Program UP Center for Integrative and Development Studies and UNICEF Manila 2005, p. 79.

[40] See Internet Child Pornography and Young People in Dakar, Abstract, available at _.

[41] See YAN HONG, XIAOMING LI, RONG MAO, BONITA STANTON, Internet Use Among Chinese College Students: Implications for Sex Education and HIV Prevention, CYBERPSYCHOLOGY& BEHAVIOR, Volume 10, Number 2, 2007, 161-170.

3.2.4 Grooming

[41] *Phenomenon*

Digital technologies such as instant messaging and Email and new social spaces in the Web, such as chat rooms, teen dating portals, online multiplayer games and social networking sites, have shaped the process of grooming a child for sexual abuse and exploitation.[42] Law enforcement cases provide important insights into new grooming approaches and vulnerabilities of children. However, research in this area lags behind technological development and youth practices and mostly predates social networking sites and virtual worlds.[43] Against this background, it is perhaps not surprising that an exploratory literature review has revealed only very limited data on grooming by adults or peers via social networking sites and similar interactive platforms in developing nations.

[42] *Anecdotal Evidence*

According to a study from Thailand, 22% of the surveyed younger children reported communicating with virtual friends, and 33% used IM and Email or chat rooms to speak with strangers. 24% of all responding seven- to eleven-year-olds have met face-to-face with someone they first met over the Internet, and in 58% of these cases, the meeting was a surprise, which turned into an unpleasant experience for half of them, mostly because their virtual friends had lied about themselves. Twenty-percent of the seven- to eleven-year-olds who used online chat mentioned shocking experiences online, mainly due to the use of bad language or because the counterpart intended to send violent or sex-related materials. Among older children, 25% of chat users reported that their correspondent had invited them to engage in sexual activities.[44] These results are supported by anecdotal evidence from other developing counties. One qualitative African study, for instance, quotes articles in popular magazines and newspapers according to which one of South Africa's popular instant messaging services is used to distribute pornography

[42] See, e.g., Deborah Muir, Violence Against Children in Cyberspace, A contribution to the United Nations Study on Violence against Children, ECPAT International, 2005, pp. 46-51.

[43] Earlier research suggested that "cases of sexual predation on minors by adults typically involved post-pubescent youth who were aware that they were meeting an adult male for the purpose of engaging in sexual activity", ISTT report, p. 4.

[44] Isabelle Michelet, Our Children at Risk Online: The Example of Thailand, in: A Survey Report, Our Children at Risk Online, The Example of Thailand, ECPAT International 2003, p. 17 and p. 24 et seq.

and allows pedophiles to contact minors, often by pretending to be minors themselves.[45]

3.2.5 Cyberbullying

Phenomenon

[43] In developed nations, online harassment and cyberbullying are the most frequent threats that children face, both online and offline. While both concepts have no clear and consistent definition and are therefore difficult to measure, a growing body of research suggests that various forms of cyberbullying happen to a significant minority of children and young people online. It frequently takes place between individuals who know one another, is often reciprocal and is often correlated with other forms of risky behavior and disconcerting psychological problems.[46]

Anecdotal Evidence

[44] Cyberbullying has also been reported from various developing nations, including South Africa, China, India, and Thailand, among others.[47] Indian scholars in particular have identified cyberbullying as an important issue, particularly among students between 7th to 12th grades.[48] A study on mobile phone bullying in India suggests that 65% of surveyed school students have been victims of mobile phone bullying, and that 60% have been involved in bullying others.[49] A 2002 survey among 1,845 college students from an eastern province of China also suggests that cyberbullying is a significant issue and links it, together with other forms of online risk behaviors such as

[45] Tanja E. Bosch, Wots ur ASLR? Adolescent girls' use of cellphones in Cape Town, April 25, 2008, p. 6 and 17 (manuscript on file with authors)

[46] See ISTTF report, p. 17.

[47] See, e.g., Shaheen Shariff, Cyber-bullying: issues and solutions for the school, the classroom and the home, Routledge (2008), pp. 54-64. See also Larry Stillman, Is there an ideal type? Developing planning and evaluation models for a digital social inclusion project: Digital Doorways, South Africa, Prato CIRN 2008 Community Informatics Conference: ICTs for Social Inclusion: What is the Reality? Refereed Paper at http://www.ccnr.net/pratoconf2008/stillman.pdf.

[48] See Debarati Halder and K. Jaishankar, Bullying and Cyber Bullying in Schools: Need to address the Legal and Policy Vacuum in India. July 2007, available at http://www.articleco.com/Article/Bullying-and-Cyber-Bullying-in-Schools--Need-to-address-the-Legal-and-Policy-Vacuum-in-India/47140; see also Debarati Halder and Jaishankar K., (2007). The problem of cyber bullying amongst school students in India: The loopholes in IT Act CyberLawTimes.com , Monthly Newsletter, volume 2, issue 8, August 2007.

[49] See Shaheen Shariff, Cyber-bullying: issues and solutions for the school, the classroom and the home, Routledge (2008), p. 63. K. Jaishankar and Debarati Halder, in: Cyber bullying among school students in India, K. Jaishankar (ed.), International Perspectives on Crime and Justice, Cambridge Scholars Publishing (2009), 579.

visiting pornographic sites, to the sexual activity level and status, respectively, of young users.[50]

3.3 Working Hypotheses

3.3.1 General Observations

State of Research

[45] An exploratory review of the literature that identifies and discusses the digital risks of children in developing nations suggests (one might add: not surprisingly given the contextual factors outlined above and resource constraints) that this strand of research—despite very important individual contributions—is relatively nascent in terms of methodologies, breadth, and depth when compared with the state of knowledge in the United States and Europe. Consequently, much of the materials referenced in the reviewed sample refer to industrialized nation studies and articles. To the extent that developing nation-specific research has been conducted, much of it appears to be based on anecdotal evidence, with only a few exceptions.

Comparability

[46] Where either qualitative or quantitative information regarding the risk categories is available, the results are typically not comparable between countries. The problem of data comparability with regard to risky behavior, however, is part of a larger issue that goes far beyond digital safety and applies not only to developing nations: While great progress has been made to standardize statistical indicators and methodologies to measure the use of information and communication technology by young people across the world, statistical comparability is still very limited.[51] With regard to future research on children and young people in digital spaces, researchers in developing nations and elsewhere may be inspired by the best practice guide for cross-national comparative research as developed by EU Kids Online project.[52]

---

[50] Yan Hong, Xiaoming Li, Rong Mao, Bonita Stanton, Internet Use Among Chinese College Students: Implications for Sex Education and HIV Prevention, Cyberpsychology & Behavior, Volume 10, Number 2, 2007, 161-170. See also Qing Li, A cross-cultural comparison of adolescents' experience related to cyberbullying, Educational Research (forthcoming).

[51] See, ITU, Use of Information and Communication Technology by the World's Children and Youth, 2008, pp. 15-18.

[52] See Sonia Livingstone and Leslie Haddon, EU Kids Online: Final Report, pp. 31-32 with reference to the online FAQ.

3.3.2 Specific Observations

Risk Categories

[47] Looking back at the framework outlined above, the exploratory literature review suggests that the most prevalent digital safety risks that children and young people face in developing nations are sexual and/or related to other forms of aggressive behavior in nature. Commercial and value oriented risks, by contrast, play a little role in the reviewed materials. Some of the most frequently mentioned sexual risk categories are well known from the industrialized world context: meeting strangers and being groomed, exposure to pornography, or creating/uploading pornographic materials (especially via mobile phones) are phenomena that are also discussed in the U.S. and across Europe. Familiar from the industrialized nations' perspective are also issues around cyberbullying, which seems to become an increasingly global risk for youth online. Similarly, sporadic reports about access to violent and hateful content highlight a problem of both developed and developing environments. However, the review also suggest issues that are of particular concern and frequency in developing-countries: The production of child abuse images and the role of the Internet in human trafficking are two risk subcategories that are emphasized in many of the reviewed developing nation reports and studies.

Differences in Detail

[48] Although the majority of the risks identified in the developing nation context are not categorically different from what studies in European countries or the U.S. have revealed, it is crucial to highlight and further explore important differences in detail. Developing policy based substantially on experience from a markedly different setting, rather than the specific context where the intervention must operate, presents challenges for both accurate risk diagnosis and effective mitigation strategy, Indeed, simply looking at the contextual factors outlined above, at least two frequently mentioned characteristics are striking: First, mobile phones and other portable digital devices (e.g. digital cameras) play a particularly prominent role within most risk subcategories. Second, in instances where computers and fixed lines are used to get online, the access environment is likely to look quite different, with shared infrastructure as provided by Internet cafés as an often-cited contextual feature. These differences in detail are reminders to be cautious with applying digital safety insights for children gained in the developed world to developing environments,

despite the relative similarity of the phenomena. That being said, it requires more research in all geographic, social, and cultural contexts to understand how these differences play out with regard to the individual risk profile of children and young people, as well as with respect to possible remedies.

4 Mapping Approaches and Strategies

4.1 Overview

Improving Safety

[49] The scholarly articles, reports, studies and other materials reviewed in the context of this exploratory paper not only identify the various issues that put children from the developing world at risk in digital contexts. Many sources also consider action that can be taken to improve digital safety for children and young people, or even include a set of recommendations. Not unlike proposals from the developed world, the suggested strategies vary significantly in approach and design. Some of them, for instance, are aimed at addressing one particular issue (e.g. child pornography). Others are more comprehensive, omnibus approaches to digital safety and seek to deal with different types of risky behaviors. Some approaches rely heavily on government interventions, while others highlight the responsibility of the private sector (like ISPs).

Illustration

[50] The next paragraphs summarize three examples of possible interventions in developing nations to further illustrate how the different approaches might look in nation-specific contexts. Many more—or different—examples could have been selected, but a comprehensive review of respective proposals is outside the scope of this exploratory study. The point here is to illustrate the variety of approaches and strategies that have been proposed or taken, and to re-emphasize the importance of contextual factors.

4.2 Examples

4.2.1 Illustration 1: Action Plan for Mauritius

Child Safety Online Action Plan

[51] As part of the National Information Security Strategy, the National Computer Board of Mauritius set up a Child Safety Online Committee, which was mandated to develop an Action Plan for Child

Safety Online. The Committee consists of government officials, members of the police, representatives of the Internet community and other organizations and has worked "to find solutions which will make the Internet a safer place for children in Mauritius without diminishing their enjoyment of the exciting opportunities which it offers."[53] The Action Plan, released in January 2009, is based on an assessment of the current state of child online safety in Mauritius, focusing on reports by various law enforcement authorities and other government units, looking into legislation in Mauritius, and surveying the international playing field. This analysis has led to a set of cross-cutting recommendations, which includes the following elements:

- Public awareness campaign (organization of Safer Internet Day; child safety online programs on TV and radio; logo drawing competition; awareness sessions for schools; women and community centers; Website, etc.);
- Safety measures for schools and public internet access points (including IT security policies and filtering tools and codes of conduct for schools; mandating "appropriate technology to deny access to inappropriate Web sites" for public internet access points and cyber cafés);
- Best Practices for ISPs (encourage ISPs to provide filtering tools; codes of conduct for voluntary compliance);
- Legislation to improve child online safety (based on the Model Legislation developed by the International Center for Missing and Exploited Children);
- Enforcement and reporting measures (sensitization of the public regarding reporting mechanisms, creation of a cyber patrol);
- International cooperation (Interpol; ratification of the UN Optional Protocol); and
- Monitoring of the Action Plan (creation of a special committee with monitoring and reporting obligations).

4.2.2 Illustration 2: Cooperation Agreement in Brazil

Cooperation Law Enforcement – Industry

[52] The Brazilian government has taken aggressive measures to combat child pornography on the Internet. NGOs have worked with

[53] See National Computer Board, Child Safety Online Action Plan for Mauritius, January 2009, available at http://www.gov.mu/portal/sites/isf/files/Final%20Action%20Plan%20version.pdf

the legislative branch and the federal prosecutors office to collect data and take action against pedophiles, and a special congressional committee has made a concerted effort to convince ISPs to cooperate with local authorities and to enter into far-reaching cooperation agreements. In 2008, an important agreement of this type was reached between the federal prosecutors of Sao Paulo and Google, whose social networking service Orkut is very popular in Brazil, but is also used to distribute child pornography. The cooperation agreement sets forth a large number of obligations, among them the following:[54]

- 180-day preservation of connection data including Email login, Internet Protocol address, access logs, data and time of connection;
- Removal of illegal content hosted on Orkut within 72 hours;
- Awareness raising activities;
- Granting communication tools for expedited communication on cyber-crimes between the federal prosecutors and the company;
- Cooperation with Safernet, a Brazilian NGO, in order to detect child pornography;
- Implementing filtering technology for detecting child pornography images;
- Bi-monthly meetings with law enforcement authorities;
- Etc.

Several of the provisions of this and analogous agreements with other ISPs have been incorporated in the bill for a controversial law on cybercrime (known as "Lei Azeredo"),[55] which is currently under consideration in Congress and has been hotly debated among privacy advocates and cyberlaw scholars.[56]

---

[54] See Gilberto Martins de Almeida, Brazil's Experience in Obtaining Cooperation from ISPs in the Fight Against Child Pornography, Project on Cybercrime, Octopus Interface Conference on Cooperation against Cybercrime, Strasbourg, 10-11 March 2009, available at http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_if09_pres_gilbertogoogle.pdf.

[55] See, e.g., Eduardo Azeredo, The 2009 Status of Brazil's legislation on the fight against cybercrime, Council of Europe Conference on Cooperation against Cybercrime, Strasbourg 10-11 March 2009, available at __.

[56] See, e.g., coverage by Diego Casaes, Brazil: Amplified conversations to fight the Digital Crimes Bill, Global Voices, June 11th, 2009, available at http://globalvoicesonline.org/2009/06/11/amplified-conversation-fighting-the-digital-crimes-bill-in-brazil/.

4.2.3 Illustration 3: China's Green Dam Youth Escort

Mandating Filtering Software

[53] A notice jointly issued in May 2009 by the Chinese Ministry of Industry and Information Technology, the Civilization Office of the Central Communist Party Committee, and the Ministry of Finance informed computer manufacturers of the Ministry's intention to require all new PCs sold in China – including those imported from abroad – to have filtering software installed. The purported intent of the software called "Green Dam Youth Escort" is "to filter harmful online text and image content in order to prevent the effects of this information on youth and promote a healthy and harmonious Internet environment."[57] Green Dam would regularly update PCs with a database of banned sites and block access to those addresses. According to the company that developed Green Dam, the software could be deactivated or uninstalled with a password. Blocked sites can be accessed either with a password allocated by an administrator or by adding addresses to a white list of allowed sites. In turn, additional URLs could be added to the black list on the user's hard drive. The company compiles and updates the blacklist of Web sites, reportedly primarily focused on pornographic sites. The software company claimed that its cooperation with a research institute of the Ministry of Public Security on image-recognition technology was limited to pornography.

[54] The Green Dam software appears to accomplish more than to protect children from harm. Tests of the software by independent researchers revealed that it is far more intrusive than any other content control software that has been reviewed. The software was designed not only to block access to a wide range of Web sites based on keywords and image processing, (including porn, gaming, gay content, religious sites and political themes), but also actively monitors individual computer behavior. As a result, programs like word processing and Email can be suddenly terminated if content algorithms detect inappropriate speech. The researchers concluded that the functionality of Green Dam goes far beyond that which is needed to protect children online, give parents little control, and subjects users to various security risks.[58] In response to massive

[57] "Notice Regarding the Pre-Installation of "Green" Online Filtering Software on Computers," Ministry of Industry and Information Technology Notice No. 226 [2009], accessed May 19, 2009 at http://tech.sina.com.cn/it/2009-06-09/17073163327.shtml.

[58] Robert Faris, Hal Roberts and Stephanie Wang, China's Green Dam: The Implications of Government Control Encroaching on the Home PC, OpenNet Initiative Bulletin, available

critique, political and industry pressure, and internal disagreement over process issues, the Minister of Industry and Information Technology announced in August 2009 that computer companies were no longer obliged to ship the software with home or business use computers, but that schools, Internet cafés and other public access computers are still mandated to run the software.

4.3 Working Hypotheses

[55] From a bird's eye perspective, the tools available for increasing digital safety for children and young people in the developing world are not categorically different from respective initiatives in developing nations. Almost all of the reviewed proposals included one or more of the following three pillars: *Toolkit*

- *Law and law enforcement*: Several of the reviewed proposals include calls for law reform. In particular, governments are often urged to introduce or improve national legislation against child pornography. Stronger law enforcement, including increased cross-border cooperation, is also a typical element in the strategy mix.
- *Technology*: Various proposals include the use of technology as a tool to improve digital safety. Filtering technologies in particular have been under consideration, both at the level of the individual access point as well as the network level. Usually, the filtering of child sexual abuse images or other forms of pornography has been in the focus.
- *Awareness and Education*: Many of the reviewed materials emphasize the importance of awareness raising campaigns targeted at parents, teachers, and children alike. Educational initiatives and school programs (media literacy curriculum) are also frequently part of the toolkit to enhance digital safety for children and young people.

Although the available tools for enhancing digital safety look similar across the world, the examples provided above—many more could be added—indicate that important contextual differences are likely to exist with regard to the specific design and usage of the respective instruments, as well as the processes—including procedural

---

at http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc.

safeguards—accompanying them. From a comparative perspective, this suggests that the transfer of "solutions" from one context to another requires a careful prior analysis of the institutional framework and the interplay among the various contextual factors outlined above, including a comprehensive stakeholder analysis.

Child Safety Rhetoric

[56] A phenomenon that can be observed in the developed world context might deserve at least as much attention in some of the less developed economies: to separate between programs that genuinely try to improve the safety of children and young people in a digital context from the merely rhetorical. The concerns are at least twofold. Depending on the respective political environment, the robustness of the legal system and other country-specific characteristics, the enhancement of child digital safety may be used as an argument to promote the application of certain (usually: more interventionist) approaches and instruments with significant spillover effects. In other instances the child digital safety theme can be "hijacked" to legitimize (often: legal or regulatory) interventions that, in fact, serve different primary purposes such as, for instance, surveillance or censorship than the references to the protection of children might suggest. The evaluation of the various approaches, strategies, and tools therefore needs to take into account a broad range of country-specific contextual factors, as indicated above.

5 Summary/Conclusion

Knowledge Gap

[57] Our relatively extensive search aimed at identifying literature on child digital safety in the developing world revealed a knowledge gap between how much is known about this topic in the industrialized nations. While the safety of children and young people in digital spaces has become an important issue of qualitative as well as quantitative research in the developed world and has led to a significant body of knowledge, the research efforts in the developing nations, with few exceptions, are still relatively early stage.

Cross-Country Analysis

[58] A brief analysis of digitally-relevant developing world characteristics suggests that various contextual factors such as technological, economic, market, educational, and cultural parameters need to be taken into account at the levels of risk analysis and risk evaluation and with regard to response strategies. This is supported by previous cross-country analyses of Internet risks

encountered by young users that underscore that this type of knowledge gap cannot be bridged by directly transferring insights from the developed to the less developed world for policymaking purposes. However, in light of very limited data from the developing world and the importance of the issue, it does seem appropriate to work with existing frameworks from the Western world as lenses for horizon scanning in order to begin to systematically identify (but not evaluate) child digital risks in the developed world.

Identifying Risks

[59] Following such a pragmatic approach, a tentative review of literature on child digital safety issues in the developing world suggests that the most prevalent risks are sexual and/or related to other forms of aggressive behavior, while commercial and value-oriented risks currently play a marginal role. Several of the most frequently mentioned sexually-oriented risk categories have also been identified in the developed world. Meeting strangers and being groomed, exposure to pornography, or creating/uploading pornographic materials are examples of such familiar forms of risky behavior. Similarly, cyberbullying seems to be an increasingly global phenomenon as several reports from the developing world indicate. However, the exploratory review also suggests issues that, according to qualitative research and based on quantitative indicators, are of particular concern in developing nations, especially the production of child abuse images and the role of the Internet in human trafficking of children.

Similarities and Differences

[60] Although many of the risks identified in the developing world bear a resemblance to phenomena that are observable in the developed world as well, it is crucial to highlight and further explore important differences in detail, such as access devices (e.g. mobile phones) and access locations (e.g. Internet cafés) in addition to possibly different usage patterns, attitudes and skill levels, among other variables. Similarly, the tools available for improving child digital safety in the developing world and encompassing regulatory, technical, policy and educational measures looks very similar to the one used in the developed world. But again, a closer look suggests important contextual differences with regard to the specific design and use of these instruments (e.g. law enforcement, filtering technology, educational campaigns, etc.) that call for a careful analysis of the particular ecosystem before recommendations are formulated or specific measures propagated, especially in countries where the legal and institutional framework is nascent or not otherwise not robust (e.g. lack of rule of law).

[61] These findings demonstrate, first and foremost, the need for more research and capacity building, both in the developing and developed world. In order to foster knowledge exchange, the authors suggest the creation of a working group that seeks to address the knowledge gap identified in this exploratory study by completing a multi-lingual literature review on child digital safety issues in the developing world, identifying and mapping initiatives, organizations, and individual researches in the field, and making all data available on an open, collaborative online platform. Such an initiative should focus on a small number of countries to start with, but can be expanded over time. In addition to research and capacity building, the authors propose, following the pragmatic approach outlined in this paper, selected field experiments in collaboration with UNICEF and local partners as test beds aimed at improving child online safety based on the information we already have. One envisioned project, among others, could focus on the use of mobile phones in particular regions with the goal of developing a "mobile app" for children and young people that helps them to identify and manage risky behaviors in digital contexts.

Next Steps