



ESCWA
United Nations Economic and Social Commission for Western Asia


Global Models for Protection of Children Online and the Path Forward for the Arab Region

Matthew Perkins, IT Officer



Presentation Plan


- Policies and Data
- Scenarios
- Implications for the Arab Region
- Discussion



Policy Drivers

- What drives policy?
- What should drive policy?


Hypothesis: Perception of risk, particularly by parents



Case Study: China

- In 2007, 70% of the user population is under age 30 and almost 60% are men.
- The penetration rate in urban areas is about 20%, compared with just over 3% in rural areas.
- Among occupations, students make up nearly a third of Chinese internet users, and business workers account for 30% more. The rest are a mixture of self-employed, non-profit workers, the unemployed, teachers, government workers, and army personnel.


China's Online Population Explosion, What It May Mean for the Internet Globally... and for U.S. Users, Pew 2007



Case Study: China

- “Internet users thought internet use could lead to several bad outcomes: About six in ten, 61%, thought internet users could easily become addicted to the internet, and the same number thought users could easily be affected by online pornography. More than two-fifths, 43%, said the internet could lure users into making the wrong kind of friends, and another 42% said internet use easily presented risks to personal or private information.”
- “These negative impressions were significantly stronger among non-users: 72% were concerned about pornography, 81% about internet addiction, 66% about making the wrong kind of friends, 55% about risks of exposing personal information.”
- “93% of internet users said they considered much of internet content to be unsuitable for children.”

China's Online Population Explosion, What It May Mean for the Internet Globally... and for U.S. Users, Pew 2007




Case Study: China

Why are the Chinese principally worried about Internet use addiction?

- “When asked which online content they thought should be controlled, more internet users targeted the most offensive or annoying content: 87% of internet users would control or manage pornography; 86% violent content; 83% spam or junk mail; 66% advertisements; 64% slander against individuals.”
- “Fewer respondents targeted the very popular but less malicious entertainment and recreation opportunities. Half of respondents said online games should be controlled, and more than one in four (27%) said online chatting should be controlled.”


China's Online Population Explosion, What It May Mean for the Internet Globally... and for U.S. Users, Pew 2007



Case Study: China


- “According to findings from the fourth and most recent of a series of surveys about internet use in China from 2000 to 2007, over 80% of respondents say they think the internet should be managed or controlled, and in 2007, almost 85% say they think the government should be responsible for doing it.”

China's Online Population Explosion, What It May Mean for the Internet Globally... and for U.S. Users, Pew 2007



Case Study: United States

- The problem of inaccurate public perceptions of risk addressed directly by researchers.



CRIMES
AGAINST
CHILDREN
RESEARCH
CENTER

1 in 7 Youth: The Statistics about Online Sexual Solicitations


Janis Wolak
David Finkelhor
Kimberly Mitchell
Crimes against Children Research Center
December 2007

Are 1 in 7 youth threatened by "online predators"?

Articles about online dangers frequently cite statistics from a 2005 University of New Hampshire study that 13% of youth were sexually solicited by online predators. (This statistic is sometimes referenced as coming from the National Center on Missing and Exploited Children, which funded and published the study).

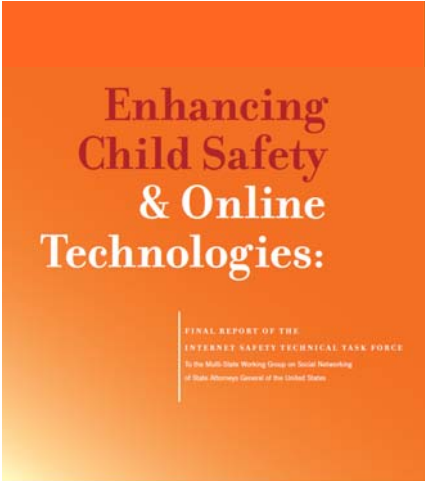
As the authors of the research upon which these numbers are based, we believe these statistics often have been misunderstood. The following points are important caveats that those using or quoting this statistic need to understand in order to avoid further confusion.

- 1) **These solicitations did not necessarily come from "online predators".** They were all unwanted online requests to youth to talk about sex, answer personal questions about sex or do something sexual. But many could have been from other youth. In most cases, youth did not actually know the ages of solicitors. When they believed they knew, they said about half were other youth.
- 2) **These solicitations were not necessarily devious or intended to lure.** Most were limited to brief online comments or questions in chatrooms or instant messages. Many were simply rude, edgy comments like, "What's your bra size?"
- 3) **Most recipients did not view the solicitations as serious or threatening.** Two-thirds were not frightened or upset by what happened.
- 4) **Almost all youth handled unwanted solicitations easily and effectively.** Most reacted by blocking or ignoring solicitors, leaving sites, or telling solicitors to stop.




Case Study: United States

- Internet Safety Task Force



DECEMBER 31, 2008


Berkman
Center for Internet & Society



Case Study: United States

“...cases typically involved post-pubescent youth who were aware that they were meeting an adult male for the purpose of engaging in sexual activity. ...Youth report sexual solicitation of minors by minors more frequently, but these incidents, too, are understudied, underreported to law enforcement, and not part of most conversations about online safety.”


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, December 31, 2008



Case Study: United States

“The Internet increases the availability of harmful, problematic and illegal content, but does not always increase minors’ exposure. Unwanted exposure to pornography does occur online, but those most likely to be exposed are those seeking it out, such as older male minors. Most research focuses on adult pornography and violent content, but there are also concerns about other content, **including child pornography and the violent, pornographic, and other problematic content that youth themselves generate.**” (emphasis added)

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, December 31, 2008



Case Study: United States

“Youth identify most sexual solicitors as being other adolescents (48%; 43%) or young adults between the ages of 18 and 21 (20%; 30%), with few (only 4%; 9%) coming from older adults and the remaining being of unknown age (Finkelhor et al. 2000; Wolak et al. 2006). Not all solicitations are from strangers; 14% come from offline friends and acquaintances (Wolak et al. 2006, 2008b). Youth typically ignore or deflect solicitations without experiencing distress (Wolak et al. 2006); 92% of the responses amongst Los Angeles–based youth to these incidents were deemed “appropriate” (Rosen et al. 2008). Of those who have been solicited, 2% have received aggressive and distressing solicitations (Wolak et al. 2006). Though solicitations themselves are reason for concern, few solicitations result in offline contact. Social network sites do not appear to have increased the overall risk of solicitation (Wolak et al. 2008b);...”


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, December 31, 2008



Case Study: United States

“The risk profile for the use of different genres of social media depends on the type of risk, common uses by minors, and the psychosocial makeup of minors who use them. Social network sites are not the most common space for solicitation and unwanted exposure to problematic content, but are frequently used in peer-to-peer harassment, most likely because they are broadly adopted by minors and are used primarily to reinforce pre-existing social relations.”


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, December 31, 2008



Case Study: United States

“Minors are not equally at risk online. Those who are most at risk often engage in risky behaviors and have difficulties in other parts of their lives. The psychosocial makeup of and family dynamics surrounding particular minors are better predictors of risk than the use of specific media or technologies.”


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, December 31, 2008



Case Study: United States


“In online contexts, perpetrators may appear to be anonymous, but this does not mean that the victims do not know the perpetrators or that the victims are not able to figure out who is harassing them. Wolak et al. (2006) found that 44% know the perpetrator offline, but Hinduja and Patchin (2009) found that 82% know their perpetrator (and that 41% of all perpetrators were friends or former friends).”

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, December 31, 2008



Case Study: United States

- Implications:
- There are many misconceptions regarding risks facing children online.
- Predation is not as widespread as believed.
- Child pornography and cyber bullying are most often perpetrated by minors.



Case Study: United States

Cyberspace is not a uniformly risky zone.
Children more at risk in real life are more at risk in cyberspace.


Socio-economic factors are a greater predictor of online risk than access availability indicators.



Case Study: European Union

Meta-study with broad participation and active support from EU Member countries.






Case Study: European Union

Classification system for assessing risk and actors across the spectrum.

| Online risks | Providers' motives | | | |
|--|--|------------------------------------|---|--|
| | Commercial | Aggressive | Sexual | Values |
| Content Child as recipient | Advertising, spam, sponsorship | Violent/hateful content | Pornographic or unwelcome sexual content | Racism, biased or misleading info/ advice (e.g. drugs) |
| Contact Child as participant | Tracking/harvesting personal information | Being bullied, harassed or stalked | Received unwanted sexual comments, being groomed, meeting strangers | Self-harm, unwelcome persuasion |
| Conduct Child as actor | Illegal downloads, hacking, gambling | Bullying or harassing another | Sending or posting porn, sexual harassment | Providing advice e.g. suicide/pro-anorexic chat |

Hasebrink, U., Livingstone, S., Haddon, L. and Ólafsson, K. (2009) Comparing children's online opportunities and risks across Europe: Cross-national comparisons for EU Kids Online. LSE, London: EU Kids Online (Deliverable D3.2, 2nd edition) ISBN 978-0-85328-406-2




Case Study: European Union

High degree of variability in the nature of online risk among and between EU countries.


| | % Online teenagers in Europe | | |
|---|------------------------------|-------------------|--------------------|
| | Estimated median | Lowest % reported | Highest % reported |
| Sexual content (child as recipient): Seen pornographic or unwelcome sexual content | 40% | 25% | 80% |
| Sexual contact (child as participant): Received unwanted sexual comments | 25% | 6% | 56% |
| Met online contact offline | 9% | 6% | 20% |
| Aggressive content (child as recipient): Seen violent or hateful content | 32% | 15% | 90% |
| Aggressive contact (child as participant): Been bullied/ harassed/ stalked | 18% | 10% | 52% |
| Aggressive conduct (child as actor): Sent bullying/ harassing messages | 12% | 8% | 18% |
| Additionally, a risk associated with most contact risks: Given out personal information | 50% | 13% | 90% |

Hasebrink, U., Livingstone, S., Haddon, L. and Ólafsson, K. (2009) Comparing children's online opportunities and risks across Europe: Cross-national comparisons for EU Kids Online. LSE, London: EU Kids Online (Deliverable D3.2, 2nd edition) ISBN 978-0-85328-406-2



| | 1) Child has encountered harmful content (%) | 2) Child knows what to do in situations, which make them feel uncomfortable (%) | Correlation between encounters with harmful content and coping (within countries) (r)* |
|----------------|--|---|--|
| EU 25 | 30.8 | 66.0 | -.02 |
| Bulgaria | 59.3 | 46.2 | .11 |
| Estonia | 57.7 | 45.4 | -.19 |
| Slovenia | 57.5 | 61.7 | -.04 |
| Sweden | 54.9 | 63.7 | -.27 |
| Poland | 49.7 | 55.9 | .02 |
| Czech Republic | 49.7 | 60.1 | .02 |
| Austria | 45.0 | 66.4 | .08 |
| Netherlands | 41.8 | 71.3 | -.24 |
| Denmark | 38.5 | 68.4 | -.14 |
| Spain | 36.3 | 51.0 | .14 |
| Portugal | 33.6 | 47.5 | .18 |
| Ireland | 28.3 | 63.6 | .10 |
| Greece | 27.4 | 54.8 | .05 |
| Belgium | 26.6 | 64.2 | -.19 |
| Italy | 24.7 | 68.0 | -.19 |
| Germany | 23.2 | 70.8 | -.01 |
| United Kingdom | 21.9 | 75.4 | -.12 |
| Cyprus | 19.0 | 72.4 | .35 |
| France | 18.3 | 68.9 | .02 |

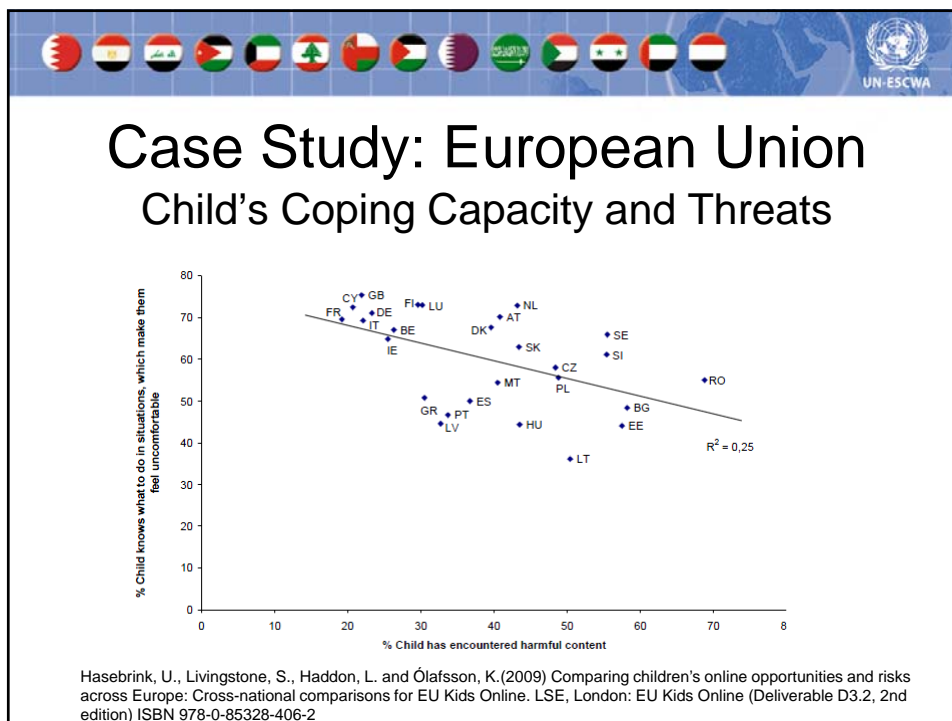
Hasebrink, U., Livingstone, S., Haddon, L. and Ólafsson, K. (2009) Comparing children's online opportunities and risks across Europe: Cross-national comparisons for EU Kids Online. LSE, London: EU Kids Online (Deliverable D3.2, 2nd edition) ISBN 978-0-85328-406-2



Case Study: European Union

Encounters with harmful or illegal content

| | At home | At school |
|----------------|---------|-----------|
| Austria | 7 | 5 |
| Belgium | 20 | 3 |
| Bulgaria | 3 | 4 |
| Cyprus | 5 | 3 |
| Czech Republic | 11 | 7 |
| Denmark | 22 | 14 |
| Estonia | 17 | 4 |
| France | 11 | 0 |
| Germany | 7 | 3 |
| Greece | 10 | 3 |
| Iceland | Nd | nd |
| Ireland | 6 | 1 |
| Italy | 8 | 8 |
| Netherlands | 31 | 9 |
| Norway | Nd | nd |
| Poland | 11 | 6 |
| Portugal | 8 | 2 |
| Slovenia | 20 | 9 |
| Spain | 14 | 2 |
| Sweden | 34 | 16 |
| The UK | 12 | 4 |
| EU 25 | 12 | 5 |



Case Study: European Union


“It can be concluded that those who belong to higher SES groups are generally exposed to fewest risks. Further, middle SES groups experience more risk and lower SES groups experience the most. It seems likely that several factors are at work here, with the relatively lesser access of the lowest status groups resulting in less exposure to risk, thus complicating the correlation between SES and risk. It is noteworthy too that the Irish report finds that only 41% of lower SES parents monitor their children's internet use, compared with 81% of other groups, and that children from lower SES groups are more likely to have access to computers and the internet in their bedroom than higher SES groups (Downey, Hayes, & O'Neill, 2007). Lower parental monitoring may, it seems, be associated with – possibly result in – greater exposure to risk among children.”

Hasebrink, U., Livingstone, S., Haddon, L. and Ólafsson, K. (2009) Comparing children's online opportunities and risks across Europe: Cross-national comparisons for EU Kids Online. LSE, London: EU Kids Online (Deliverable D3.2, 2nd edition) ISBN 978-0-85328-406-2



Case Study: European Union


- Implications:
- Online risks vary greatly on a national level
- Online risk is significantly influenced by socioeconomic status



Scenario #1

A boy sends a girl an explicit picture by phone. She then forwards it to her sister.

Legal questions: Is the boy a child pornographer?
Should the telecommunications carrier be liable?
Did the girl distribute child pornography when she forwarded the message to her sister? Is her sister guilty of possessing child pornography?



Scenario #2

- A boy sends my daughter an explicit photo.
- Legal questions: If I take the phone from her and go to the police, have I conveyed child porn? Did I possess child pornography when I picked up the phone? Do I have immunity to convey the image when I am making the report to law enforcement?



Implications for Harmonization

International Center
for Missing and
Exploited Children,
Model Legislation
and Global
Inventory



المواد الإباحية المتعلقة
بالأطفال
التشريع النموذجي والاستعراض العالمي للتشريعات

الطبعة السادسة • 2010 •



 International Centre
FOR MISSING & EXPLOITED CHILDREN



Implications for Harmonization

- “There should be no criminal liability for children involved in pornography, and such should be clearly stated in national legislation. Regardless of whether a child is a compliant victim or a non-cooperative witness, the fact remains that he/she is a **child victim.**”
- “Criminal liability must focus on the adult offender, who is responsible for the exploitation of the child, and on the crimes he/she committed against that child.”
- “Legal provisions should be enacted that would allow for protections of the child victim as a witness in any judicial proceedings that may occur, including permitting closed-circuit testimony in certain circumstances and establishing guidelines for the presence of victim advocates in the courtroom.”


Child Pornography: Model Legislation & Global Review,
Copyright © 2010, International Centre for Missing & Exploited Children.



Implications for Harmonization

“Finally, the last group consists mostly of ISPs, credit card companies, and banks. In many circumstances, law enforcement would never know about many child pornography offenses if ISPs did not report them (either voluntarily or under legal obligation). Given the heavy traffic in child pornography over the Internet, ISPs are in an almost ideal position to report suspected child pornography offenses to law enforcement. A “notice and takedown” requirement should be enacted within national legislation, and consideration should be given to **statutory protections that would allow ISPs to fully and effectively report child pornography, including the transmission of images, to law enforcement or another designated agency.**”
(emphasis added)

Child Pornography: Model Legislation & Global Review,
Copyright © 2010, International Centre for Missing & Exploited Children.



Implications for Harmonization

- Form policy on actual, not perceived risks
- Reality often doesn't match expectations
- Similar variances among and between Arab states and EU member countries, implies variance in usage would also be seen. Cultural similarities
- Regional model which builds-in accommodation of nation level variance



Legislative Models

- International Center for Missing and Exploited Children
- ESCWA Cyber Legislation Harmonization Directives
- ITU Policy Framework



UN-ESCWA

Global Policy Framework Guidelines

حماية الأطفال
على الخط

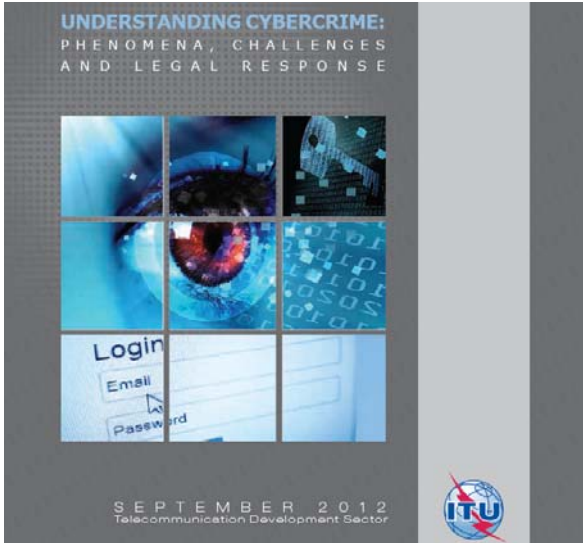


ITU

UN-ESCWA

International Inventory

UNDERSTANDING CYBERCRIME:
PHENOMENA, CHALLENGES
AND LEGAL RESPONSE




SEPTEMBER 2012
Telecommunication Development Sector

ITU



Further Action:

- Specific research on usage and risk patters for Arab youth
- Regionally harmonized, locally sensitive approach to protection



Path Forward

- Global policy framework on cyber legislation and protection of children
- Global models seem to imply the problems are the same cross-culturally.
- What are the nuances of Arab youth usage patterns?

