BEYOND BORDERS INC.

Au-Delà Des Frontières Inc.

Ensuring Global Justice for Children

Winnipeg Toronto Vancouver Ottawa

Head Office: 387 Broadway, Winnipeg, MB R3C 0V5
Tel: (204) 284-6862 **Fax:** (204) 452-1333 www.beyondborders.org

What ISPs Should and Could Do To Prevent Child Sexual Exploitation

What is an Internet Service Provider (ISP)? An ISP "is a business organization that offers users access to the Internet and related services. In the past, most ISPs were run by the phone company. Now ISPs can be started by just about anyone. They provide services such as Internet transit, domain name registration and hosting, dial-up or DSL access, leased line access and colocation."[1]

What are some of the threats that the Internet poses to children?

Child pornography: A child pornography image is a permanent record of a child's sexual abuse. Some experts estimate that there are approximately 14 million pornographic websites with some posting approximately one million child abuse images.[2] In March 2006, 40 people in Canada, the United States, England and Australia were charged in relation to a massive Internet child pornography ring that involved trading pictures and live video of children being sexually abused and raped. The victims were between 18 months and 11 years old, and at least four were from Edmonton.

Exposure to adult pornography: Besides pornography available to children on PCs, expansion of the adult porn industry through emerging video technology in cell phones, iPods and other hand-held devices threatens to make it easier for children to access adult content. When Apple announced an iPod with video playback capabilities, many adult entertainment companies announced that they would make video programming available in the player's format. The sale of adult entertainment for downloading to cell phones is a multimillion-dollar business in Europe,[3] and in North America it is rapidly expanding. The "Mobile Adult Content Congress" took place in Miami in January 2006, with speakers from Virgin Mobile UK and Vodafone.[4] In November 2005, the cell phone industry in the United States announced plans to adopt a rating system, but critics note that this simply allows the industry to offload responsibility for monitoring content onto parents, and that children are often much quicker to pick up on

[1] "Internet Service Provider," online: Wikipedia <http://en.wikipedia.org/wiki/Internet_service_provider>.
[2] "Internet Based Sexual Exploitation of Children and Youth Environmental Scan," online: National Child Exploitation Coordination Centre <http://ncecc.ca/enviroscan_2005_e.htm>.
[3] Mike Musgrove, "Porn becomes a big draw on little gadgets" *The Washington Post* (19 November 2005) 4.
[4] Mike Musgrove, "Technology's Seamier Side; Fates of Pornography and Internet Businesses Are Often Intertwined" *The Washington Post* (21 January 2006) D.01.

technology than parents are.[5]

Luring: As defined by the *Criminal Code*, luring refers to using a computer for the purpose of facilitating the commission of the offence of sexual exploitation against someone who is under 18.[6] There have been countless Canadian arrests for this offence in recent years. In June 2006, 32-year-old Jean-Pierre Nafekh of Villeray, Quebec, was sentenced for attempting to lure who he thought was a 12-year-old girl in a chat room into having sex for the first time.[7]

Webcams: Many young teens get undressed in front of a webcam, believing that the person on the other end will keep the images private, only find out later that these images are circulated widely. In the summer of 2005, two young teenage girls from Edmonton thought they were using chat rooms to communicate with friends when they were dared to expose themselves in front of their web cameras. Following this, the girls received the message: "I am not who you think I am." The message was followed by threats that that image would be shared and posted on the internet unless the girls participated in more explicit, fully nude sexual activity in front of the webcam.[8]

What can and should ISPs do to help prevent the sexual exploitation of children?

1. Use a filtering system to restrict access to child pornography sites. Since 2004 British Telecom has used **"Cleanfeed"**, a system that blocks child pornography sites from its 2.7 million Internet subscribers by filtering out either specific domain names or the unique numeric addresses associated with the web server hosting the site. Lists are supplied and updated by the Internet Watch Foundation, an industry monitoring group.[9]

Critics argue that such filtering amounts to censorship because it could cause legitimate sites to be blocked and an ISP could easily add other categories to its blocked list.[10] British Telecom has no plans to expand the project beyond child pornography sites, however, and there is an appeals process for sites that believe they are wrongly blocked.[11]

ISPs that adopt any filtering system should use all reasonable measures to prevent legitimate sites from being blocked. While filtering creates a small risk of infringing upon freedom of expression, this risk is greatly outweighed by the large effect it could have on protecting children.

2. Restrict underage users of mobile devices from accessing adult content. In Britain, wireless networks bar adult content to mobile devices by default. To lift the restriction, a user must provide proof that he or she is over 18.[12]

---

[5] "Control phone porn" *The Gazette* (12 November 2005) A.30.
[6] *Criminal Code*, R.S.C. 1985, c. C-46 s. 172.1.
[7] Monique Beaudin, "Crown wants jail term for Internet luring: Man thought he was chatting with preteen" *The Gazette* (9 June 2006) A.8: What he thought was a 12-year-old girl turned out to be a police officer.
[8] Natalie Alcoba, "Porn hacker had 100 victims" *The Gazette* (29 July 2006) A.10.
[9] "U.K. ISP plans to block online kiddie porn," online: CTV <http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20040607/BT_childporn_20040607?s_name=&no_ads=>.
[10] "Doubts over web filtering plans," online: BBC News <http://news.bbc.co.uk/2/hi/technology/3797563.stm>.
[11] *Supra* note 9.
[12] *Supra* note 5.

3. Moderate chatrooms and other interactive services in which children are likely to participate. The UK Home Office recommends that public interactive communication providers undertake a risk assessment of the potential their service has to harm children. If there is a risk to children, then they should employ moderation, which involves a person or technical filter being responsible for reviewing content posted by users. Technical moderation attempts to filter words and phrases it has been programmed to identify, and telephone and e-mail addresses. However, it can be outwitted by the creative use of combinations of numbers, letters and punctuation marks. Human moderation is more effective and can be employed in a variety of ways; content can be reviewed before it becomes visible to other users, after it becomes visible, a sample of content can be reviewed, or moderation can take place only after a request for intervention is made.[13]

Providers should assess what level of risks their respective interactive services pose to children and determine what levels of monitoring are appropriate.

4. Make sure that child protection mechanisms keep pace with technological advancements. As internet service provision is constantly evolving, new threats to children will emerge. When ISPs introduce new technology, they should do it responsibly and with the proper safeguards in place for children.

Should ISPs be legislated into doing something more? Currently the CRTC does not regulate content on the internet. The justification given is that "appropriate tools for dealing with what may be offensive already exist. These include Canadian laws, industry self-regulation, content-filtering software, and increased media awareness."[14]

Dr. Max Taylor of University College Cork, Ireland, argues that ISPs have a duty to exercise social responsibility, because it is not acceptable in any other commercial setting to facilitate the committing of a crime. However, he also notes that some ISPs have used the defence of being a "common carrier" of information, a claim used by the mail industry to protect itself from being sanctioned for contributing to the distribution of illegal material.[15]

Beyond Borders takes the position that ideally, ISPs will self-regulate themselves and legislation will be unnecessary. If this does not happen, however, legislation would be appropriate. Legislation could force ISPs to engage in standard minimum practices, and as long as these were sufficiently upheld then the ISPs would not be held liable for any illegal content that they unknowingly distributed. In the United States, federal law requires ISPs to report suspected transmissions of child pornography to the National Centre for Missing and Exploited Children. Some members of Congress have suggested that the industry either needs to do more or face stricter legislation.[16]

---

[13] "Home Office Task Force on Child Protection on the Internet," online: Home Office (UK) <http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/moderation-document-final.pdf?view=Binary>.

[14] "Internet," online: Canadian Radio-television and Telecommunications Commission <http://www.crtc.gc.ca/eng/INFO_SHT/t1003.htm>.

[15] Steven Kleinknecht, "Borders Conference – Rethinking the line: The Canada – US Border Child Pornography and the Internet Session" online: Department of Justice Canada <http://www.justice.gc.ca/en/ps/rs/rep/2001/e_border.html>.

[16] Paul McDougall, "Child Porn Fight Gets Infusion of ISPs' Expertise And Cash", *Information Week* (3 July 2006), Iss. 1096, p. 32.

One intermediate measure short of legislation would be for Canadian ISPs to set up a self-regulatory system, perhaps through the Canadian Association of Internet Providers (CAIP)[17]. Membership in this organization could be made conditional upon continued adherence to an industry-wide code of practice. The UK's Internet Services Providers' Association (ISPA) employs this strategy through its "Code of Practice".[18]

What can I do to help? First of all, sign up for ECPAT's "Make-IT-Safe" campaign at www.make-it-safe.net , an online petition to lobby IT leaders to "create a global child protection body to set and implement global industry standards, research safety technologies and fund a global educational campaign", among other goals.

Locally, you can find out whether your ISP engages in child-friendly practices, and if not, demand that they do. If possible, consider switching services to a company that is part of the solution rather than the problem.

Recommendations:

1. Membership in a Canadian ISP regulatory system should be made contingent upon ISPs having to retain data for many years, as law enforcement officials are often frustrated when investigating crimes against children to find that the needed information is no longer available.

2. Civil litigation legislation should be amended to allow for law suits against those who expose children to unwanted sexual material.

3. Use a filtering system such as "Cleanfeed" to restrict access to child pornography sites.

Update – December 17, 2007: "Project Cleanfeed Canada" was launched in late 2006. Under this program Cybertip.ca creates and maintains a regularly updated list of specific foreign-hosted Internet addresses associated with images of child sexual abuse and provides this list in a secure manner to participating ISPs. The ISPs' filters then prevent access to these addresses.[19] This program is voluntary, yet as of November 2006 many of the big ISPS had signed on to it, including Bell and Rogers.[20]

Cybertip.ca compiles its list of offensive addresses based on complaints it receives from Canadians regarding websites that potentially host child pornography. Analysts assess these complaints and websites meeting the necessary criteria are blocked. There is an appeal process modeled after the UK's BT Cleanfeed initiative.[21]

Author: David Thompson, Third Year Student at University of Toronto, Faculty of Law
Tel: (416) 820-1274 (Cell)

[17] See http://www.cata.ca/Communities/caip/.
[18] "ISPA Code of Practice", online: ISPA UK <http://www.ispa.org.uk/about_us/page_16.html>.
[19] "Project Cleanfeed Canada Frequently Asked Questions," online: Cybertip.ca <http://www.cybertip.ca/en/cybertip/cf_faq>.

[20] "New initiative will see ISPs block child porn sites," online: CTV <http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20061123/isps_childporn_061123/20061123?hub=Canada>.
[21] *Supra* note 1.