Family
Online Safety
Institute

State of Online Safety Report

2008

A FOSI Publication

State of Online Safety Report 2008

Family
Online Safety
Institute

www.fosi.org

ISBN 978-0-9801970-0-6

Table of Contents **Page**

Preface

Stephen Balkam
CEO, Family Online Safety Institute

The state of online safety is in flux. At no time in (our brief, digital) history, have so many tools to filter, monitor and control content and behavior been available to parents, teachers, employers and other concerned adults. And yet, the flood of digital images, videos, text and sound tracks threatens to overwhelm our defenses. Governments and regulators take steps to deal with this issue with vastly varying levels of success and legality. The large, amorphous "internet industry" makes efforts to self-regulate and offer assistance and help to parents and consumers with mixed results. Parents, themselves, awaken to the realization that they have a vital and growing role to play in protecting their kids. And educators, researchers and the non-profit organizations do what they can to track, study, and respond to the new realities of our always on, digital world.

The State of Online Safety Report 2008 is our first attempt to take an international snap shot of the incredibly diverse and innovative attempts to keep kids safe online, while also respecting free expression. What began as a look at just five countries has blossomed into an account of twice that many as more and more international contributors offered their analyses. We expect that our next, annual report, will grow even larger to reflect the extraordinarily rich diversity and broad range of activity now taking place throughout the world.

What you will find here is a range of voices, statistics, examples and efforts from some of the leading experts in the field. What each writer has attempted to do is to lay out the state of online safety in their country by listing and describing current and proposed legislation, existing educational efforts and the many technology tools and devices created to help protect kids. There is also some analysis and commentary on where the trends are leading and what the writer sees as signs of optimism or concern. It is a subjective synopsis, an individual assessment of what exists and what is coming.

For if there is one recurring theme, it is the ever changing, technologically challenging, transitory-ness of this subject that makes it so invigorating and infuriating at the same time. There is no one law, no one technology, no one awareness campaign that will fix this. We are embarked on a journey without end. As we catch up with and provide solutions to technologies and content that could prove harmful to kids, new devices, new strange meeting places spring up and thwart our earlier efforts and consign them and their websites to the archives. (Have a look at some earlier attempts at www.archives.org!)

And yet, we must not give up or abdicate our responsibilities as parents, as teachers, as industry leaders or as government officials. We have a generation to guide and young lives to protect. We also must preserve our centuries old

freedom to speak and to assemble and to express ourselves in our infinitely varied ways, so that this generation of kids will inherit these rights and take on the unenviable task of protecting the next generation from whatever and wherever the new technology and the ingenuity of programmers take us.

Acknowledgements

I would first like to thank my good friend, Adam Thierer, not only for his excellent chapter on the US, but also for his early contributions and suggestions for this report. Thanks, also, to Jillian Hess for her invaluable edits, notes and queries. To my colleague, Samantha Woolfe for her tireless work editing and working with the authors on their contributions, securing the chapters you see before you and assembling the many contributions that came from many lands. And to all our contributors who have provided us a unique insight into their country's attempt to both protect kids and free expression in our ever changing online world.

Chapter I:
The United States

by Adam Thierer
Senior Fellow, The Progress & Freedom Foundation, USA

Overview

Over the past dozen years, concerns about online child safety and access to objectionable material have prompted a great deal of legislative activity in the United States. Most attempts to legislate in this area, however, have been struck down by the Supreme Court and various lower courts as a violation of the First Amendment of the Constitution. The First Amendment, which states that "Congress shall make no law… abridging the freedom of speech," has been viewed as an impediment on most attempts to directly control or curtail objectionable online speech or content.

The crucial factor cited in each of the courts' decisions is the so-called "less restrictive means" test. For example, in striking down the Communications Decency Act of 1996, which sought to ban the transmission of materials that were "obscene or indecent," the Supreme Court declared in *Reno v. ACLU* (1997) that a law which places a "burden on adult speech is unacceptable if less restrictive alternatives would be at least as effective in achieving" the same goal.[1] This "less restrictive means" test has been cited in several others cases, and US courts have rejected efforts to regulate cable television and violent video game content on similar grounds.[2]

In the short term, therefore, it appears likely that as long as there are a respectable number of private parental control tools on the market to allow families to independently control underage access to objectionable content or communications, US courts will continue to reject most efforts by lawmakers to enact regulatory solutions to child safety concerns.

Fortunately, a vibrant market of private parental control tools and methods has developed in the United States over the past decade. As will be detailed below, parents can utilize a wide variety of tools, sites, and strategies to help them decide what is acceptable in their homes for their children.

Many educational and awareness-building efforts have also been created by industry and non-profit organizations. Indeed, there are so many private efforts underway that it has become difficult to keep track of them all. The private programs and services highlighted below are only a short list of what is available.

---

[1] *Reno v. ACLU*, 521 US 844 (1997).
[2] See Adam Thierer, "Fact and Fiction in the Debate over Video Game Regulation," Progress & Freedom Foundation *Progress Snapshot* 13.7, March 2006, www.pff.org/issues-pubs/pops/pop13.7videogames.pdf

These private efforts, however, have not been matched by government efforts. Online child safety educational and awareness-building efforts are practically non-existent at the federal government level and state and local governments have only recently begun creating online safety plans and programs.

Basic Stats

- According to a March 2007 survey by the Pew Internet & American Life Project, 71 percent of all US adults use the Internet.[3]

- Another recent Pew survey noted that American teenagers were online more now than ever before. According to a Pew survey from late 2006, 93 percent of all Americans between 12 and 17 years old use the Internet. By contrast, in 2004, 87 percent were Internet users, and in 2000, 73 percent of teens were online.[4]

- Pew has also found that more than half (55%) of the 12 to 17 year old American youths use online social networking sites.[5]

- That Pew survey also revealed that parents have established a wide variety of rules for Internet use by their teenage children. The survey found that 69 percent of parents limit how much time their children can spend online and 85 percent have rules about which Internet websites they can and cannot visit.[6] The survey also noted that 74 percent of homes with teenagers have their computers in an "open family area."[7] That result was consistent with Pew surveys taken in 2004 and 2000.

- Similarly, a June 2007 poll conducted by the Kaiser Family Foundation revealed that, overall, "Parents say they are gaining control over their children's exposure to sex and violence in the media, but they remain more broadly concerned about inappropriate content in the media."[8] Specifically, the survey found that:

  - 65 percent of parents feel they closely monitor their children's media use;

---

[3] http://www.pewinternet.org/trends/User_Demo_6.15.07.htm
[4] *Ibid*.
[5] Amanda Lenhart and Mary Madden, *Teens, Privacy, and Online Social Networks*, Pew Internet & American Life Project, April 18, 2007, p. 3, http://www.pewinternet.org/pdfs/PIP_SNS_Data_Memo_Jan_2007.pdf
[6] Amanda Lenhart and Mary Madden, *Teens, Privacy, and Online Social Networks*, Pew Internet & American Life Project, April 18, 2007, p. 9, www.pewinternet.org/PPF/r/211/report_display.asp.
[7] *Ibid*, p. 8.
[8] Victoria Rideout, *Parents, Children & Media*, Kaiser Family Foundation Survey, June 2007, http://www.kff.org/entmedia/entmedia061907pkg.cfm

- 73 percent say they know a lot about what their kids are doing online;
- 87 percent check their children's instant messaging "buddy lists";
- 82 percent review their children's social networking sites; and
- 76 percent look at what websites their children have visited.

Legislation

Passed

Since 1996, the US Congress has passed a handful of measures aimed at regulating online content or activities. Some of these measures have been blocked by the courts or were considered to be in violation of the First Amendment of the Constitution.

- **Communications Decency Act (CDA) of 1996**[9]: The CDA was the first attempt by Congress to regulate objectionable material on the Internet. The law sought to ban the transmission of content over the Internet that was "obscene or indecent." The Act was immediately blocked by a lower court and a year later the Supreme Court struck down the indecency provisions of the CDA in the historical cyberlaw case of *Reno v. ACLU* (1997). The Supreme Court ruled that a law that constrains adult speech was not acceptable if the same objective could be met with less restrictive alternatives.

- **Child Online Protection Act (COPA) of 1998**: COPA was an effort by Congress to modify the CDA in response to the Supreme Court's decision in *Reno v. ACLU*. The new law sought to protect minors from harmful sexual material on the Internet by making it a crime for someone to "knowingly" place materials online that were "harmful to minors."[10] The law provided an affirmative defense from prosecution, however, for parties who made a "good faith" effort to "restrict[ ] access by minors to material that was harmful" by using credit cards or age verification schemes. The law was immediately challenged and blocked by lower courts, and it then became the subject of an epic legal battle that is still underway today.

The Supreme Court has reviewed the rule twice and in the second decision in June 2004, the Court held in *Ashcroft v. ACLU* that the law was probably unconstitutional in light of the less restrictive methods that were available to block objectionable content. Nonetheless, the case was referred back to a lower court for further review. In the most recent COPA decision, Judge Lowell Reed Jr., senior judge of the US District Court for the Eastern District of Pennsylvania, ruled that COPA remained an unconstitutional burden because it was "impermissibly vague and overbroad" and did not represent "the least restrictive, most effective alternative in achieving the compelling interest" the government

[9] http://www.epic.org/free_speech/CDA/cda.html
[10] http://www4.law.cornell.edu/uscode/html/uscode47/usc_sec_47_00000231----000-.html

had in this matter.[11] Judge Reed also held that the market for private filtering tools had continued to flourish since COPA was passed and that those filters blocked an estimated 95 percent of sexually explicit material. He also found "that there is no evidence of age verification services or products available on the market to owners of Web sites that actually reliably establish or verify the age of Internet users. Nor is there evidence of such services or products that can effectively prevent access to Web pages by a minor."[12]

Thus, the permanent injunction against the enforcement of COPA remains in effect today. The government has not announced whether it will appeal the case before the Supreme Court for a third time.

- **Children's Online Privacy Protection Act (COPPA) of 1998**: COPPA, which went into effect in April 2000, requires websites specifically marketed to children under the age of 13 to get "verifiable parental consent" before allowing children access to their sites.[13] The Federal Trade Commission (FTC), which is responsible for enforcing COPPA, adopted a sliding scale approach to obtaining parental consent.[14] This approach allows website operators to use a variety of methods to comply with the law, including print-and-fax forms, follow-up phone calls and e-mails, and credit card authorizations. The FTC also authorized four "safe harbor" programs operated by private companies that help website operators comply with COPPA.[15] In a recent report for Congress, the FTC said that no changes to COPPA were necessary at this time because it had "been effective in helping to protect the privacy and safety of young children online."[16] In discussing the effectiveness of the parental consent methods, however, the agency said that "none of these mechanisms is foolproof" and that "age verification technologies have not kept pace with other developments, and are not currently available as a substitute for other screening mechanisms."[17]

- **Children's Internet Protection Act (CIPA) of 2000**: The Children's Internet Protection Act of 2000 was another attempt by Congress to enact limitations on objectionable online materials in the wake of court challenges to the CDA and COPA. CIPA was far narrower in scope than those previous regulatory efforts since it only applies to schools or libraries receiving federal funding on the "E-rate" system, a program that subsidizes communications and computing

[11] http://www.techliberation.com/COPA_decision.pdf
[12] http://www.techliberation.com/COPA_decision.pdf
[13] http://www.coppa.org/coppa.htm
[14] See: Federal Trade Commission, *How to Comply with The Children's Online Privacy Protection Rule*, November 1999, www.ftc.gov/bcp/conline/pubs/buspubs/coppa.htm
[15] The four safe harbor programs are administered by the Children's Advertising Review Unit of the Council of Better Business Bureaus ("CARU"); the Entertainment Software Rating Board (ESRB); TRUSTe; and Privo.
[16] Federal Trade Commission, *Implementing the Children's Online Privacy Protection Act: A Report to Congress,* February 2007, p. 1, www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf
[17] *Ibid.*, p. 12-13.

technology for schools and libraries. Under CIPA, if schools and libraries wish to continue receiving E-Rate assistance, they must certify that they have an Internet safety policy and technology protection measures in place to block or filter Internet access to pictures that are obscene or harmful to minors.[18] Unlike the CDA and COPA, CIPA was upheld by the US Supreme Court as constitutional in June 2003.[19]

Proposed in the 110th Congress (2007-2008)

The following bills related to online safety or Internet regulation have been introduced in the 110th Congress. All descriptions are taken from the US Library of Congress website.[20]

- H.R. 1008 – "**Safeguarding America's Families by Enhancing and Reorganizing New and Efficient Technologies Act of 2007**" (Representative Melissa Bean, Illinois) or the "SAFER NET Act" requires the FTC to establish an Office of Internet Safety and Public Awareness (the Office) to be headed by a Director. The FTC, acting through the Office, is obligated to carry out a nationwide program to increase public awareness and education regarding Internet safety, which utilizes existing resources and efforts of all levels of government and other appropriate entities. The program initiatives include: evaluating and improving the efficiency of existing Internet safety efforts; identifying and promoting best practices; establishing and carrying out a national outreach and education campaign; serving as the primary contact in the federal government and as a national clearinghouse for Internet safety information; facilitating access to, and the exchange of, such information; providing expert advice to the FTC; and providing technical, financial, and other appropriate assistance to Internet safety entities.

Rep. Bean reintroduced the Safer Net Act in August 2007 as H.R. 3461. The new bill is a more narrowly drawn measure that only instructs the FTC to carry out a nationwide program to increase public awareness and provide education to promote safer Internet use. The newer measure does not require that the FTC provide grants or take any additional steps as was envisioned under the original measure.

- S.1086 – "**Cyber Safety for Kids Act of 2007"** (Senators Max Baucus, Montana and Mark Pryor, Arkansas) provides stronger protections for parents regarding their children's access to sexually explicit material over the Internet. This act, which was formerly known as S.2426 - the Cyber Safety for Kids Act of 2006, was rejected by the previous Congress. It was reintroduced by its original sponsors on April 11, 2007.

[18] http://www.fcc.gov/cgb/consumerfacts/cipa.html
[19] http://www.supremecourtus.gov/opinions/02pdf/02-361.pdf
[20] http://thomas.loc.gov/

- S. 49 – "**Protecting Children in the 21st Century Act**" (Senator Ted Stevens, Alaska): This Act amends the Communications Act of 1934, which requires the Federal Communications Commission (FCC) to issue regulations requiring video services to prevent child pornography. The Crime Control Act of 1990 would be amended to triple the fines on providers of electronic communication services or remote computing services who knowingly and willfully fail to report child pornography. It also requires warning labels for websites depicting sexually explicit material.

The bill also includes the "**Deleting Online Predators Act of 2007**," which was a stand-alone measure in the previous session of Congress. This proposes amending the Communications Act of 1934 to require schools and libraries that receive universal service support to enforce a policy that: prohibits access to a commercial social networking website or chat room unless used for an educational purpose with adult supervision; and protects against access content harmful to minors, such as obscene visual depictions and child pornography. The Act directs the FCC to issue a consumer alert regarding use of the Internet by child predators and to establish a website resource. (This was also proposed under H.R. 1120. sponsored by Representative Mark Kirk, Illinois)]

Finally, S. 49 also proposes the "**Children's Listbroker Privacy Act**," (Senators Ron Wyden, Oregon and Ted Stevens, Alaska) proposes making it unlawful to: sell personal information about individuals under age 16; purchase personal information about an individual identified by the seller as a child for the purpose of marketing to that child; and use personal information for any practice that violates certification terms.

- S. 602 – "**Child Safe Viewing Act of 2007**" (Senator Pryor) obligates the FCC to initiate proceedings to consider measures to encourage or require the use of technologies, which are compatible with various communications devices or platforms, that can improve or enhance the ability of a parent to protect his or her child from any indecent or objectionable video or audio programming (as determined by the parent).

- H.R. 837 – "**Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act**," or the "SAFETY Act of 2007" (Representative Lamar Smith, Texas) amends the federal criminal code to prohibit: financial transactions in interstate or foreign commerce that facilitate access to, or the possession of, child pornography; and Internet content hosting providers or email service providers from facilitating access to, or the possession of, child pornography.

- H.R. 668 – "**Web Video Violence Act**" (Representative Mario Diaz-Balart, Florida) amends the Omnibus Crime Control and Safe Streets Act of 1968 to reduce funding for states which fail to prove that their laws or official policies require increased penalties for a criminal defendant, who is convicted of a violent

crime, for placing a video or image of the commission of the crime on the Internet.

- S.431 (and H.R. 719) – "**Keeping the Internet Devoid of Sexual Predators Act of 2007**" or the "KIDS Act of 2007" (Senators John McCain, Arizona and Chuck Schumer, New York) amends the Sex Offender Registration and Notification Act to require a convicted sex offender to: include in the National Sex Offender Registry any electronic mail address, instant message address, or other similar identifier used to communicate over the Internet; and keep such information up-to-date.

- S. 519 (and H.R. 876) – "**Securing Adolescents From Exploitation Online Act of 2007**" (Senator McCain), also know as the "SAFE Act of 2007", amends the federal criminal code to expand the reporting requirements of electronic communication and remote computing service providers with respect to violations of child sexual exploitation and pornography laws.

- S. 1965 – "**Protecting Children in the 21st Century Act**" (Senator Ted Stevens, Alaska and Senator Daniel Inouye, Hawaii). Like H.R. 3461, this bill instructs the FTC to carry out a nationwide program to increase public awareness and provide education to promote safer Internet use. Another section of the bill deals with the reporting and prosecution of child pornography.

Education and Awareness Efforts

Government Education or Awareness Efforts

In the US, government efforts to promote online safety education or awareness have been largely uncoordinated among various agencies and programs. One notable exception at the federal level has been the On Guard Online website, a collaboration of six federal agencies, which "provides practical tips from the federal government and the technology industry to help you be on guard against Internet fraud, secure your computer, and protect your personal information."[21] Although the initiative does not focus exclusively on parental controls or online child protection, it does offer some helpful tips in that regard. The effort includes a "Stop-Think-Click" promotion that recommends "Seven Practices for Safer Computing." Additionally, the Federal Bureau of Investigation (FBI) offers similar tips on its "Parent's Guide to Internet Safety" website.[22] However, as mentioned above, these efforts are largely uncoordinated and receive very little promotion from federal agencies or congressional lawmakers.

[21] http://onguardonline.gov/index.html The six agencies are the Federal Trade Commission, the Department of Commerce, the Securities and Exchange Commission, the US Postal Inspection Service, the Office of Justice Programs, and the Department of Homeland Security.
[22] www.fbi.gov/publications/pguide/pguidee.htm

Legislation was introduced this year in both the Senate and House of Representatives that would better coordinate and expand online safety education and efforts at the federal level. S. 1965, the "Protecting Children in the 21st Century Act," was introduced by Senator Ted Stevens (R-Alaska), Vice Chairman of the Senate Commerce Committee and Committee Chairman Daniel Inouye (D-Hawaii). The House measure, H.R. 3461, the "Safeguarding America's Families by Enhancing and Reorganizing New and Efficient Technologies Act of 2006," or "SAFER NET" Act, was introduced on August 4th by Rep. Melissa Bean (D-IL).

Both bills would require that the Federal Trade Commission (FTC) "carry out a nationwide program to increase public awareness and provide education" to promote safer Internet use. "The program shall utilize existing resources and efforts of the Federal Government, State and local governments, nonprofit organizations, private technology and financial companies, Internet service providers, World Wide Web-based resources, and other appropriate entities, that includes—

> (1) identifying, promoting, and encouraging best practices for Internet safety;
>
> (2) establishing and carrying out a national outreach and education campaign regarding Internet safety utilizing various media and Internet-based resources;
>
> (3) facilitating access to, and the exchange of, information regarding Internet safety to promote up to-date knowledge regarding current issues; and,
>
> (4) facilitating access to Internet safety education and public awareness efforts the Commission considers appropriate by States, units of local government, schools, police departments, nonprofit organizations, and other appropriate entities."

Some states have also proposed comprehensive online safety education initiatives. Most notably, in September 2006, the Commonwealth of Virginia produced a report entitled "Guidelines and Resources for Internet Safety in Schools."[23] The Virginia Department of Education published this report to "assist school divisions in three areas: writing an Internet safety component as part of the acceptable use policy; integrating Internet safety into the curriculum; and fostering responsibility among all stakeholders to help protect young people from online dangers."[24]

Industry-led Education or Awareness Efforts

[23] www.doe.virginia.gov/VDOE/Technology/OET/internet-safety-guidelines-resources.pdf
[24] http://www.pen.k12.va.us/VDOE/Technology/OET/internet-safety-guidelines-resources.pdf

Additionally, several major private or industry-led consumer education efforts are under way to help families learn more about parental controls and online child safety efforts.

- **ConnectSafely.org**[25] is a project of Tech Parenting Group, a nonprofit organization based in Palo Alto, Calif., and Salt Lake City, Utah. The project is the brainchild of Larry Magid of SafeKids.com and Anne Collier of NetFamilyNews.org, two of the leading experts on online child safety issues in America. The site features helpful articles and videos, safety tips, interactive forums, and commentaries. The forum allows parents and teens to interact with online child safety experts. The effort is supported by a wide variety of high-technology companies.

- **GetNetWise.org**[26] is a public service website operated by the nonprofit Internet Education Foundation,[27] which is supported by a wide array of Internet and computer companies, as well as a host of public interest organizations and child and family activists.[28] GetNetWise's website offers a comprehensive "Online Safety Guide" and lengthy inventory of "Tools for Families" that can be custom-tailored to the needs and values of individual families.[29]

- **Internet Keep Safe Coalition**[30] consists of 49 state governors or their spouses, law enforcement officials, the American Medical Association, the American Academy of Pediatrics, and many other corporations,[31] as well as private associations (including many of the groups and sites listed below) that are dedicated to helping parents, educators, and caregivers by providing tools and guidelines to teach children how to safely use technology. iKeepSafe uses an animated mascot named Faux Paw the Techno Cat to teach children the importance of protecting personal information and avoiding inappropriate places on the Internet. The organization's website offers a downloadable "10 Common Questions about Internet Safety" pamphlet[32] and several video tutorials to help parents set up various filters or controls.[33]

---

[25] www.connectsafely.org
[26] www.getnetwise.org
[27] www.neted.org
[28] Major corporate supporters include Dell, Microsoft, Verizon, Amazon.com, Yahoo!, AOL, AT&T, Comcast, Eathlink, Visa, Wells Fargo, and the RIAA. Key public interest organizations include the Center for Democracy and Technology, the American Library Association, the Children's Partnership, People for the American Way Foundation, the National Consumers League, Net Family News, ProtectKids.com, SafeKids.com, and Wired Patrol.
[29] See http://kids.getnetwise.org/safetyguide and http://kids.getnetwise.org/tools
[30] www.iKeepSafe.org
[31] Corporate sponsors include AOL, Dell, Disney, Intel, Oracle, Siebel Systems, Symantec, and Yahoo!, among others.
[32] www.ikeepsafe.org/iksc_partners/symantec/10_questions/Assets/TenCommonQuestions.pdf
[33] www.ikeepsafe.org/PRC/videotutorials/index.php

- **i-SAFE Inc.**[34] is a nonprofit foundation whose mission is "to educate students on how to avoid dangerous, inappropriate, or unlawful online behavior. This is accomplished through dynamic K-12 curriculum and community outreach programs to parents, law enforcement, and community leaders." It claims that it is the only Internet safety foundation to combine these elements.[35] i-SAFE receives federal grants to support its efforts. The organization produces several monthly newsletters, including one for parents ("i-PARENT Times") and one for educators ("i-EDUCATOR Times"), and it sells a wide variety of printed materials on online safety issues for classroom use.

- **Net Smartz Workshop**[36] is produced by the National Center for Missing and Exploited Children and the Boys and Girls Clubs of America. This comprehensive website contains web safety tips and educational materials for parents, preteens, teens, educators, and law enforcement officials. They also sponsor a site[37] devoted to younger children that features interactive online safety games and videos, as well as the NetSmartz Internet Safety Helpdesk[38], which is sponsored by the Qwest Foundation.

- **Pause-Parent-Play**[39] is an organization that offers an array of websites and services that parents can use to learn more about the media their children might want to see, hear, or play. The effort is sponsored by a diverse coalition of companies and associations, including: Wal-Mart, the Girl Scouts, the YMCA, Microsoft, Comcast, Time Warner, News Corp., the Electronic Software Association, Viacom, NBC Universal, MPAA and the Recording Industry Association of America (RIAA). The coalition's website features numerous links answering questions about how TV ratings and screening tools work (like the V-Chip and cable and satellite set-top boxes).[40] The links provided on the Pause-Parent-Play website help parents better understand how to use these and other technologies. There's also a "Get the Facts" section on the site that offers detailed explanations of how many of the current rating systems work.[41]

- **PointSmart, ClickSafe**[42] was established in July 2007 by the National Cable & Telecommunications Association (NCTA), which represents roughly 90 percent of all cable households nationwide. Under the new initiative, NCTA's member companies "pledge to help parents, families, customers and consumers create a better, safer online media environment and foster a better understanding and working knowledge of the digital media landscape."[43] The NCTA's efforts are

[34] www.iSafe.org
[35] www.iSafe.org/channels/?ch=ai
[36] www.netsmartz.org
[37] www.netsmartzkids.org
[38] www.netsmartz411.org
[39] http://pauseparentplay.org
[40] http://pauseparentplay.org/see/index.php#tv
[41] http://pauseparentplay.org/facts
[42] www.pointsmartclicksafe.org
[43] www.pointsmartclicksafe.org

being coordinated online through a website that contains interactive tips, manuals, and public service announcements to assist and educate parents and children. The new effort complements two other important undertakings that the cable industry has operated for several years: "Control Your TV"[44] and "Cable in the Classroom."[45] The "Control Your TV" initiative's website coordinates the cable industry's parental control efforts aimed at the video programming side of their business. "Cable in the Classroom" is an impressive media literacy initiative that also provides broadband connectivity and educational programming to schools and libraries for classroom use.

- **Project Online Safety**[46] is a collaborative online portal that offers a directory of online safety tools and educational materials developed by technology companies, media organizations and nonprofits. Coalition members include: AT&T, BlogSafety.com, Cable in the Classroom, Charter, Comcast, Cox, Facebook, Fox Interactive Media (owner of MySpace), Internet Education Foundation, National Cable and Telecommunications Association, Network Solutions, Qwest, Time Warner Cable, and the National Center for Missing and Exploited Children. Each organization provides an overview of its online safety efforts and links to various resources that parents can use to keep their kids safe online or to educate them about online dangers.

- **StaySafe.org**[47] is an educational website sponsored by the Microsoft Corporation "intended to help consumers understand both the positive aspects of the Internet as well as how to manage a variety of safety and security issues that exist online."[48] The site contains specific sections for teenagers, parents, senior citizens, and educators with tips and tools tailored to each group.

- **Take Parental Control**[49] is a public service website provided by Playboy Enterprises. It features parental control fact sheets for a wide variety of media, including: television, cable, cell phones, video games, and Internet surfing. The website also features a useful glossary of terms describing various technologies and parental control tools. Public service announcements are included as well.

- **WebWiseKids**[50] is a nonprofit organization "committed to teaching children and their caregivers strategies for safe Internet use, including methods of detecting and deterring online predators."[51] It specializes in interactive software and games that teach kids how to spot online threats and how to deal with them promptly.

---

[44] http://controlyourtv.org
[45] www.ncta.com/ContentView.aspx?contentId=2695
[46] www.projectonlinesafety.com
[47] www.staysafe.org
[48] www.staysafe.org/about.html
[49] http://takeparentalcontrol.org
[50] www.wiredwithwisdom.org
[51] www.wiredwithwisdom.org/who_we_are.asp

- **Wired Safety**[52] bills itself as "the largest online safety, education and help group in the world. We are a cyber-neighborhood watch and operate worldwide in cyberspace through our more than 9,000 volunteers worldwide."[53] The site offers educational services and online assistance, in addition to reviewing family-friendly websites, filtering software, and other Internet services. Wired Safety also operates or works with several other affiliated online safety sites, such as:

  - **Wired Cops**[54] are "specially-trained volunteers [who] patrol the Internet looking for child pornography, child molesters and cyberstalkers."
  - **Wired Kids**[55] is geared toward youngsters and teens to help them deal with and understand online threats.
  - **Teen Angels**[56] is "a group of 13 to 18 year-old volunteers that have been specially trained by the local law enforcement, and many other leading safety experts in all aspects of online safety, privacy, and security. After training for six sessions, the Teenangels run unique programs in schools to spread the word about responsible and safe surfing to other teens and younger kids, parents, and teachers."
  - **Net Bullies**[57] aims to protect kids from cyber-bullying.

Many other websites offer parents and kids advice about how to stay safe online, including: Net Family News,[58] ProtectKids.com,[59] SafeKids.com,[60] SafeTeens.com,[61] BlogSafety.com,[62] ChatDanger.com,[63] StopCyberbullying.org,[64] Cyberbully.org,[65] and StopTextBully.com.[66] The popular technology website CNet.com also offers a user-friendly portal[67] for families.

Technology

A wide array of technological tools and services exist in the United States for dealing with potentially objectionable online content. These tools and services will be divided into five categories: operating system filters and web browser

[52] www.wiredsafety.org
[53] www.wiredsafety.org/information/about_us.html
[54] www.wiredcops.org or www.cyberlawenforcement.org
[55] www.wiredkids.org
[56] www.teenangels.org
[57] www.NetBullies.com
[58] http://netfamilynews.org/index.shtml
[59] http://protectkids.com
[60] www.safekids.com
[61] www.safeteens.com
[62] www.blogsafety.com
[63] www.chatdanger.com
[64] www.stopcyberbullying.org
[65] www.cyberbully.org
[66] www.stoptextbully.com
[67] www.cnet.com/2001-13384_1-0.html

controls; PC-based filters & monitoring software; ISP-based filters; search engine filters; and kid-based portals and other sites geared toward kids.

Operating System Filters and Web Browser Controls

Increasingly, companies like Microsoft and Apple are integrating parental controls into computer operating systems and web browsers. As Walter Mossberg of *The Wall Street Journal* notes, these are "powerful tools to help parents get a handle on their children's computing and online activities."[68] For example, the new Windows Vista operating system is Microsoft's first version of Windows that incorporates embedded family safety tools. As Seth Schiesel of *The New York Times* reports, "With Vista, Microsoft has for the first time built a robust set of parental controls directly into the operating system, not just for gaming but also for Web browsing, file downloading and instant messaging."[69]

Vista lets parents establish "administrator" accounts and then oversee the individual users who are using the PCs. Parents can then configure the Vista sub-accounts to enable various parental control features and monitoring tools. They can turn on web filters that will block specific types of potentially objectionable website content or downloads. Limits can also be established to restrict when or how long the child may use the computer.

Also, much like new video game consoles, Vista enables parents to restrict video games by rating or title, and games with no ratings can be blocked entirely if the parents so desire. Additionally, parents can see an "activity list" of the sites their child has visited, or attempted to visit, as well as files and applications that have been downloaded. Applications or software that the parents find objectionable can then be blocked from that same screen.[70] Importantly, once these parental controls have been enabled within Vista, there is no need for parents to configure additional controls within Internet Explorer. Vista controls all Internet Explorer web-browsing activities.

Finally, Microsoft has opened up "application programming interfaces" (APIs) to third-party software developers so that they can build supplementary parental control tools in addition to the embedded Vista tools. One of these developers is IMSafer.[71] A number of other add-ons for Internet Explorer also let parents add more layers of controls. A list of these extra controls can be found at a special webpage Microsoft has created.[72]

---

[68] Walter S. Mossberg, "You Have Weapons in Your Computer to Monitor Your Kids," *Wall Street Journal*, June 14, 2007, p. B1.
[69] Seth Schiesel, "For Parents, New Ways to Control the Action," *New York Times*, January 8, 2007, www.nytimes.com/2007/01/08/arts/08vist.html?ex=1325912400&en=3bb7bc1b6a470a23&ei=5090&partner=rssuserland&emc=rss
[70] www.microsoft.com/windowsvista/features/forhome/safety.mspx#more
[71] http://www.imsafer.com/
[72] www.windowsmarketplace.com/category.aspx?bcatid=837&tabid=1

Apple's parental controls are not quite as sophisticated as Microsoft's Vista's. Apple's Safari web browser uses a white-listing approach to parental controls. This means that parents can establish which websites children can visit by bookmarking them for their kids and all other sites will be blacklisted.[i] Apple's Tiger operating system also allows parents to establish accounts for their children and control some of their online activities. In addition, parents can build a restricted "buddies list" for their children and then disallow instant messaging to anyone else. The system can also hide the child's online status so that only those pre-approved buddies can see when they are online.[73]

PC-based Filters and Monitoring Tools

Many parents are familiar with Internet filtering software and use filters to control their children's online surfing activities. At a minimum, these software tools let parents block access to adult websites and impose time management constraints on their children's computer and Internet usage.

Increasingly, however, these software packages also include far more robust monitoring tools that let parents see each website their children visit, view every e-mail or instant message they send and receive, or even record every word that they have typed.[74] Many of these monitoring tools can then send parents a periodic report summarizing their child's Internet usage and communications. More robust software programs even allow parents to capture screen shots of sites their kids have visited. Finally, these tools let parents do all the tracking in a surreptitious fashion as once the software is installed on a child's computer it is entirely invisible to the user.

Similarly, "IMSafer" offers a free downloadable tool that can help parents monitor instant messenger conversations and notify them when their child is engaged in a potentially dangerous conversation on IM.[75] Importantly, the IMSafer tool respects a child's privacy and does not allow parents to read the full transcripts of online communications. Instead, the application only monitors IM conversations for content that is considered dangerous. This includes the trading of phone numbers or other personal information.

Some parents might flinch at this level of child surveillance, but others will find it entirely appropriate, especially for very young children just starting to use the Internet.[76] Regardless, a wide variety of such filtering and monitoring tools is

[73] www.apple.com/macosx/features/family

[74] See Jessica E. Vascellaro and Anjali Athavaley, "Foley Scandal Turns Parents Into Web Sleuths," *Wall Street Journal*, October 18, 2006, p. D1.

[75] www.imsafer.com

[76] With regard to monitoring software, the National Research Council report concluded: "[A]ctive supervision of children is often appropriate—not because they are criminals but because it is the responsibility of adults to teach them how to internalize the appropriate values and to become better at avoiding inappropriate behavior as they mature." Computer Science and

available and they can be adjusted to meet parents' specific needs and values. A comprehensive list of these software tools can be found at the GetNetWise.org website,[77] but some of the most popular filtering and monitoring tools can be found below in Exhibit 1.

Exhibit 1: Internet Filtering and Monitoring Software

Activity Logger (www.softactivity.com)
BeNetSafe (www.benetsafe.com)
Bsafe Online (http://bsafeonline.com)
Children's Internet (www.thechildrensinternet.com)
Clean Internet.com (http://cleaninternet.com)
Content Cleaner (www.contentpurity.com)
Content Protect (www.contentwatch.com)
CyberPatrol (www.cyberpatrol.com)
Cyber Sentinel (www.cybersentinel.com)
CyberSitter (www.cybersitter.com)
eBlaster (www.spectorsoft.com)
FamiLink (www.familink.com)
Family Cyber Alert (www.itcompany.com)
FilterGate (http://filtergate.com)
FilterPak (www.surfguardian.net/products.shtml)
Guardian Monitor (www.guardiansoftware.com)
IamBigBrother (www.iambigbrother.com)
IM Safer (www.imsafer.com)
Internet4Families (www.i4f.com)
iShield (www.guardwareinc.com)
K9 Web Protection (www.k9webprotection.com)
KidsNet (www.sti.net/s-kidsnet.html)
McAfee Internet Security Suite (http://us.mcafee.com)
Microsoft Live One Care (www.windowsonecare.com)
NetIntelligence (www.netintelligence.com)
Netsweeper (www.netsweeper.com)
NetMop (www.netmop.com)
NetNanny (www.netnanny.com)
Norton Internet Security (www.symantec.com/home_homeoffice/products)
Online Safety Shield (www.onlinesafetyshield.com)
Optenet PC (www.optenetpc.com)
Parental Control Bar (www.wraac.org)
PC Tattletale (www.pctattletale.com)
Razzul (www.kidinnovation.com)
SafeEyes (www.safeeyes.com)
Sentry At Home (www.sentryparentalcontrols.com)
Sentry Remote (www.sentryparentalcontrols.com)
Snoop Stick (www.snoopstick.com)
Spector Pro (www.spectorsoft.com)
Spy Agent (www.spytech-web.com/software.shtml)
Surf On the Safe Side (www.surfonthesafeside.com)
SurfPass (www.cogilab.com/us/homeedition)
Webroot Child Safe (www.webroot.com)

Telecommunications Board, National Research Council, *Youth, Pornography, and the Internet* (Washington, DC: National Academy Press, 2002), p. 315.
[77] See www.getnetwise.org

WebWatcher (www.awarenesstech.com/parents/index.html)

ISP-based Filters and Tools

Stand-alone or "PC-based" filtering solutions, such as those described above, dominated the online parental controls marketplace in the late 1990s. The market has changed significantly since then, however. Today, Internet service providers (ISPs), which include major broadband service providers (BSPs), offer parental control services as part of an integrated suite of security tools, which typically also includes anti-virus, anti-spyware, and anti-spam tools. These security options are often offered free of charge, or for a small additional fee, when subscribers sign up for a monthly Internet service. Furthermore, most of these integrated tools offer automatic updates, making up-to-date protection very easy for consumers.

This means that millions of parents now have free or quite inexpensive Internet parental control tools at their disposal as soon as they sign up for Internet access through an ISP. Of course, parents can also add on other tools or independent filtering and monitoring solutions such as those outlined earlier. Exhibit 2 below lists the Internet security websites for major ISPs and broadband operators.

Exhibit 2: Internet Security and Parental Control Websites for Major ISPs and Broadband Operators

AOL (http://daol.aol.com/parentscentral)
AT&T (www.att.com/safety) and (www.att.com/smartlimits)
Cablevision (www.powertolearn.com/internet_smarts/index.shtml)
Charter (www.charter.com/Visitors/NonProducts.aspx?NonProductItem=65)
Comcast (www.comcast.net/security)
Cox (www.cox.com/takecharge/internet_controls.asp)
Earthlink (www.earthlink.net/software/free/parentalcontrols)
Insight BB (www.insightbb.com/pcsecurity/default.aspx)
Microsoft (www.microsoft.com/protect)
NetZero (www.netzero.net/support/security/tools/parental-controls.html)
Qwest (www.incredibleinternet.com)
Time Warner (www.timewarnercable.com/centralny/products/internet/parentalcontrols.html)
Verizon (http://netservices.verizon.net/portal/link/main/safety)

Search engine filters

Parents can also use tools embedded in search engines to block a great deal of potentially objectionable content that children might inadvertently stumble upon during searches.

For example, Google offers a SafeSearch feature that allows users to filter unwanted content. Users can customize their SafeSearch settings by clicking on the Preferences link to the right of the search box on the Google.com

homepage.[78] Users can choose "moderate filtering," which "excludes most explicit images from Google Image Search results but doesn't filter ordinary web search results," or "strict filtering," which applies the SafeSearch filtering controls to all search engine results.

Similarly, Yahoo! has a SafeSearch tool that can be found under the "Preferences" link on the My Web tab.[79] Like Google, Yahoo! allows strict or moderate filtering. Microsoft's Live Search works largely the same way.[80] Other search engine providers such as AltaVista,[81] AskJeeves,[82] HotBot,[83] Lycos,[84] and AllTheWeb,[85] also provide filtering tools. Working in conjunction with other filters, these search engine tools are quite effective in blocking a significant amount of potentially objectionable content.

Kid-based Portals and other Sites Geared Toward Kids

There are also many search engines and web portals geared toward younger audiences. Several excellent options, such as those listed in Exhibit 3, let kids search numerous sites without stumbling upon adult-oriented material.[86] They direct children to sites and information that are educational and enriching. In essence, these search portals are white lists of acceptable sites and content that have been pre-screened to ensure that they are appropriate for very young web surfers. The only downside of using such services is that a lot of wonderful material available on the web might be missed. Nevertheless, many parents will likely be willing to make that trade-off since they desire greater protection for their children from potentially objectionable content.

Exhibit 3: Kid-Friendly Internet Search Engines and Portals

ALA's Great Web Sites for Kids (www.ala.org/greatsites)
AOL for Kids (US) (http://kids.aol.com)
AOL for Kids (Canada) (http://canada.aol.com/aolforkids)
Ask Jeeves for Kids (www.askforkids.com)
Awesome Library for Kids (www.awesomelibrary.org)
Diddabdoo (www.dibdabdoo.com)
Education World (www.education-world.com)
Fact Monster (www.factmonster.com)
Family Source (www.family-source.com)
FirstGov for Kids (www.kids.gov)

[78] www.google.com/intl/en/help/customize.html#safe
[79] http://myweb.yahoo.com
[80] http://search.msn.com/settings.aspx
[81] www.altavista.com/web/ffset?ref=/
[82] www.ask.com/webprefs
[83] www.hotbot.com/prefs_filters.asp
[84] http://search.lycos.com/adv.php?query=&adf=
[85] www.alltheweb.com/customize?backurl=Lw&withjs=1
[86] This lists builds on the excellent compendium of sites listed at the Search Engine Watch website: http://searchenginewatch.com/showPage.html?page=2156191

KidsClick (www.kidsclick.org)
NetTrekker (www.nettrekker.com)

SearchEdu.com (www.searchedu.com)
Surfing the Net with Kids (www.surfnetkids.com)
Surf Safely.com (www.surfsafely.com)
TekMom's Search Tools for Students (www.tekmom.com/search)
ThinkQuest Library (www.thinkquest.org/library)
Yahoo! Kids (http://kids.yahoo.com)

The child-friendly web portals discussed above generally direct children to informational and educational sites and resources. However, there are many other ways to tailor the web-surfing experience to a family's specific needs and values. The Internet is full of wonderful sites dedicated to kids and teens. Many have an educational focus, while others offer enjoyable games and activities for children. Exhibit 4 highlights some of the best examples of these websites, but this list just scratches the surface. If parents wanted they could configure their web browsers to access only sites such as these and then block access to all other webpages.

Exhibit 4: Child- and Teen-Oriented Websites

Clever Island (www.cleverisland.com)
Disney Playhouse (http://disney.go.com/playhouse/today/index.html)
Disney's Club Blast (http://disney.go.com/blast)
Disney's Toon Disney Games (http://psc.disney.go.com/abcnetworks/toondisney/games)
Disney Toontown Online (http://play.toontown.com)
Habbo (www.habbo.com)
HBO Family Games (www.hbofamily.com/games)
JuniorNet (www.juniornet.com)
Kaboose Family Network (www.kaboose.com)
Kaboose FunSchool (http://funschool.kaboose.com)
KidsClick (www.kidsclick.org)
KidsFirst (www.kidsfirst.org)
Microsoft At School (www.microsoft.com/education/atschool.mspx)
Net Smartz Kids (www.netsmartzkids.org)
Nickelodeon Games (www.nick.com/games)
Nick Jr. Games (www.nickjr.com)
Nicktropolis (www.nicktropolis.com)
Noggin Games (www.noggin.com/games)
PBS Kids (http://pbskids.org/go)
Safe Sites for Children (U.K.) (www.ssfchildren.co.uk)
Surfing the Net with Kids (www.surfnetkids.com)
Surf USA (www.surfonthenet.com)
Yahoo! Kids (http://kids.yahoo.com)
Zeeks (www.zeeks.com)

Future Trends

Despite the proliferation of these online safety tools, sites, and strategies, many policymakers and other critics in the United States still protest that children are exposed to an unacceptable amount of offensive material on the Internet, mostly of a sexually explicit nature. These critics typically argue that regulation is needed because filters are not 100 percent effective in blocking pornography or other types of objectionable online content.

This raises the question of what can be counted as "success" when it comes to online filtering and blocking controls. During a recent trial about the merits of the Child Online Protection Act of 1998, the US Department of Justice (DOJ) introduced evidence showing that major Internet filters blocked sexually explicit content 87.4 to 98.6 percent of the time.[87] The DOJ seemed to suggest in its ruling that this was not sufficient. However, it is unlikely that government regulation could produce a better track record, especially due to the fact that domestic regulations are largely powerless in terms of controlling offshore activity. Private filters, by contrast, can capture objectionable offshore material. Private filters can also use industry standard identification systems to allow legitimate rated commercial content to be seen while screening out unknown or unrated content. Moreover, new methods, such as image-recognition technologies, are being developed and deployed to monitor and identify content, which will further facilitate screening and filtering.

Regardless, calls for regulation of online networks and content will continue. As illustrated above, legislative and regulatory proposals in the US show no sign of abating. If lawmakers insist on 100 percent perfection as the standard, they will never be satisfied with private self-regulation solutions such as those detailed above.

Incidentally, compared to many other countries, there hasn't been as much concern about violent material or hate speech online. That may be changing, however. Efforts are currently underway in Congress and at the Federal Communications Commission to regulate violent video programming shown over broadcast, cable or satellite television networks. This could lead to calls for similar regulations for violent programming visible on Internet websites or other interactive networks. Similarly, although hate speech has never been regulated in the United States, concerns about online "cyber-harassment" or "cyber-bullying" could prompt calls for rules governing offensive hate speech.

With regard to the future, the near term battles will continue to be preoccupied with government efforts to impose "community standards" regulation on the Internet and online communications. This will include an effort to regulate mobile

[87] *American Civil Liberties Union v. Gonzales*, No. 98-5591 (E.D. Pa. Mar. 22, 2007). For a breakdown of how successful various filters were, see http://www.aclu.org/freespeech/internet/27490res20061120.html

platforms and social networks. However, if lawmakers hope to succeed in this effort, they will need to find a way to prove to the courts that private solutions (parental controls, filters, monitoring tools, content tailoring efforts, etc.) are largely ineffective at blocking underage access to objectionable material. Challenges to the legitimacy and effectiveness of private controls and filters have been underway for many years, but the intensity of these attacks has been stepped up over the past year. This is part of a concerted effort by many lawmakers and critics to discredit the "less restrictive means" test that the courts have relied on when striking down regulatory enactments.

If this effort fails, and it is likely that it will based on previous regulatory attempts' limited success, critics really only have two diametrically opposed options left to consider. First, they could push for an amendment to the US constitution that would seek to weaken the protections afforded by the First Amendment. These protections have proven so strong that there are discussions taking place now of traditional "community standards" regulation giving way to almost absolute First Amendment protection of online expression, potentially even for sexually "obscene" content. Amending the US Constitution is a drastic step, however, that would encounter fierce resistance and take years to execute. It is very difficult to imagine that proponents could clear the very high hurdles that lie in their path,[88] especially since they would be seeking to modify the First Amendment of the Constitution, which many Americans consider sacrosanct.

The second alternative would entail major ongoing expenditures for nationwide online safety awareness and educational campaigns. Unfortunately, as pointed out above, very little media literacy instruction is being carried out within America's educational system at any level today. For the most part, media literacy and online safety awareness lessons are not routinely integrated into the curricula at elementary schools, secondary schools, high schools, or colleges. This situation could easily be reversed if US officials were willing to utilize more resources on media literacy and online safety awareness efforts. However, it remains to be seen if lawmakers and critics will be willing to take this path. Regulation, not education, continues to dominate most discussions about online child safety in the United States.

---

[88] Amending the US Constitution is fairly difficult and time-consuming. Article V of the Constitution provides two processes by which amendments can be proposed and approved. (1) Congress proposes the amendment: Both houses of Congress approve by two-thirds votes a resolution calling for the amendment. The resolution does not require the president's signature. To come into effect, the proposed amendment must then be "ratified" or approved by the legislatures of three-fourths of the states. Congress typically places a time limit of seven years for ratification by the states. (2) The states propose an amendment: The legislatures of two-thirds of the states vote to call for a convention at which constitutional amendments can be proposed. Amendments proposed by a convention would again require ratification by the legislatures of three-fourths of the states. For more detailed information, see: http://www.lexisnexis.com/constitution/amendments_howitsdone.asp http://www.usconstitution.net/constam.html

In the meantime, however, private tools and methods for curtailing access to potentially objectionable online materials or communications continue to proliferate. And non-profit and industry-led education and awareness efforts offer a great deal of beneficial assistance to parents looking to keep their children safe in online environments.

Chapter II:
United Kingdom

by Chris Holder
Family Online Safety Institute and Partner, Brand X, UK

The Internet Landscape in the UK

A lot has changed in the last ten years since the media started reporting about the Internet and broadband. Now two thirds of Britons have access to high-speed Internet at home,[89] and there are more than 10.7 million broadband connections and 99.9 percent coverage in the UK, which is the best level of any country in the G8.[90]

Public perception of the Internet has changed too. No longer is it seen as something for computer geeks or just a way to send emails; it now acts as a channel to access and share a growing range of information and communication services. So much so that the majority of broadband users now spend on average more than nine hours a week online with two thirds (65 percent) logging on daily.[91]

Over the last twelve months, users have gone beyond basic services, such as online shopping and banking. The UK's Office of Communications (Ofcom)[92] has carried out research which shows that 43 percent of people with broadband have used websites as a means to keep in touch with people, and over the last 12 months, the UK has been gripped by the rise of social networking sites such as Facebook and MySpace. To give an example of the extent of the social networking revolution, there are now more than one million members of the London Facebook network alone.

In addition to creating and sharing content online via their social networking pages, 14 percent of Internet users have contributed material to a website or blog, and 11 percent of Internet users have their own webpage or blog.[93]

Around half of all broadband users have accessed online media content, with a quarter listening to audio or watching downloaded video clips on a weekly basis.

---

[89] Dutton, W. and Helsper, E.J., "The Internet in Britain: 2007," Oxford Internet Institute, University of Oxford (Oxford, UK), 2007, p. 8, www.oii.ox.ac.uk/research/oxis/OxIS2007_Report.pdf.
[90] BT Group plc, "The BT Story," August 31, 2007, http://www.btplc.com/Thegroup/Companyprofile/TheBTstory/TheBTstory.htm.
[91] Ofcom, "The Communications Market: Broadband Digital Progress Report," April 2007, p. 21, http://www.ofcom.org.uk/research/cm/broadband_rpt/broadband_rpt.pdf. Viewed on October 5, 2007.
[92] http://www.ofcom.org.uk/
[93] "The Communications Market: Broadband Digital Progress Report," p. 1.

Use of all these services was much higher among the 16 to 24 year olds, confirming their position at the forefront of new media take-up. Seven in ten have used online audio, almost two in three have watched and downloaded video clips, and 35 percent have viewed longer video content such as feature films and full television programmes via a broadband connection. The majority of young adults are also contributors of online content, with 65 percent having uploaded their own pictures or photos. Of these 16 to 24 year olds, more females than males have uploaded static content.[94]

The UK and Online Child Safety

The UK is leading the world in online safety, with the government, law enforcement agencies and industry itself (Internet service providers and software vendors) working together on a range of initiatives to make the Internet a safer place and to catch criminals online.

Safety has always been an important element of the Internet, even before it became mainstream. This stems back as far as 1996, with the formation of the Internet Watch Foundation (IWF) which was the result of an agreement between the government, police and the Internet industry that a partnership approach was needed in order to tackle the growing problem of child abuse images being distributed online. The IWF is the only authorized 'hotline' in the UK for the general public to report their inadvertent exposure to illegal content on the Internet to and is funded by EU and the UK Internet industry agencies including Internet service providers (ISPs), mobile network operators and manufacturers, content service providers (CSPs), telecommunications and software companies, and credit card bodies.

Additionally, the Home Secretary's Internet Task Force for Child Protection on the Internet (ITFCPI)[95] brings together the Internet industry, child welfare organisations, the police and government. It was established in March 2001 in response to a general election, media pressure after the death of Sarah Payne by Carole Vorderman, and a report by the Internet Crime Forum, which made several recommendations for protecting children on the Internet, including improved supervision of chat rooms and better displayed safety messages.

Also coming out of the Task Force was the Child Exploitation and Online Protection Centre (CEOP)[96] which provides a single point of contact for the public, law enforcers and the communications industry to report targeting of children online and offers advice and information to parents and potential victims of abuse 24 hours a day.

[94] "The Communications Market: Broadband Digital Progress Report," p. 23.
[95] http://police.homeoffice.gov.uk/operational-policing/crime-disorder/child-protection-taskforce
[96] http://www.ceop.gov.uk/

CEOP also took over the work of the Paedophile Online Investigation Team (POLIT)[97], which was created in January 2003 as a part of the nationally agreed strategy to combat child abuse on the Internet and which was to provide a single point of contact in the UK. POLIT was involved in reactive and proactive investigations and undertook research, assessments and dissemination of intelligence on behalf of UK law enforcement agencies. Another key area of POLIT is the development of ChildBase, a sophisticated database of all images ever seized, that was created to assist with the identification of both the victims and their abusers. Specialist software also allows the database to detect if the victim or abuser is known to other law enforcement agencies.

The National Crime Squad, now part of the Serious Organised Crimes Agency (SOCA)[98], and CEOP also contributed to numerous national and international committees and was the chair of the Virtual Global Taskforce (VGT)[99].

The VGT was created in 2003 as a direct response to lessons learned from investigations into online child abuse around the world. It is an international alliance of law enforcement agencies, including the Australian High Tech Crime Centre, the National Crime Squad for England and Wales, the Royal Canadian Mounted Police, the US Department of Homeland Security, and Interpol. It also has industry partners, such as AOL, BT, MSN and Vodafone.

The VGT has run a number of initiatives to help make the Internet a safer place, including "Operation PIN"[100]. This initiative involves the creation of a website that maintains that it contains images of child abuse but which, in fact, is a law-enforcement site. Anyone who enters the site and who attempts to download images sees a page that tells them they have entered a law enforcement website and committed an offence, and that their details may have been recorded and passed to the relevant national authorities.

The Internet industry also plays a key role in making the Internet a safer place for users. BT, for example, works closely with governments, law enforcement agencies, charities, ISPs, and software vendors across the globe. It has also developed a number of initiatives to educate and help protect users when they are online.

---

97 http://www.leics.police.uk/departments/3_crime_support/40_paedophile_and_online_investigation_team/

98 http://www.soca.gov.uk/

99 http://www.virtualglobaltaskforce.com/

100 Information on "Operation PIN" is available at: http://www.virtualglobaltaskforce.com/what_we_do.asp.

Internet Statistics

General Internet

- There are 10.7 million broadband connections in the UK.[101]
- 66 percent of households currently have access to the Internet, up from 58 percent in 2003.[102]
- More than 13 million UK homes and small and medium-sized enterprises (SMEs) are now connected to broadband, compared with 9.9 million in 2006 and 330,000 in 2001.[103]
- 63 percent of adults with broadband at home use it daily, while 30 percent go online at least once a week. Broadband users spend an average of 9.1 hours a week online compared to 4.4 hours for narrowband users.[104]

Internet Content

- 51 percent of adults with broadband at home have accessed online video clips, with 26 percent watching them weekly.[105]
- 43 percent of adults with broadband at home have uploaded images to the Internet and 15 percent have uploaded video content at least once.[106]

Internet Misuse

- In 2006 the Internet Watch Foundation hotline processed 31,776 reports, a 34 percent increase on 2005.
- Less than 1 percent of child abuse content has been hosted in the UK since 2003.
- The IWF's database contains 10,656 individual URLs containing child abuse content, which is a 74 percent increase from 2005; 3,077 domains account for all these URLs, with 1,667 of these domains being commercial websites.
- 10.5 percent of all URLs with child abuse content in 2006 were on photo album websites.
- 62 percent of commercial child abuse domains are hosted in the US.
- 28 percent of commercial child abuse domains are hosted in Russia.

[101] BT Group plc, "The BT Story," August 31, 2007, http://www.btplc.com/Thegroup/Companyprofile/TheBTstory/TheBTstory.htm
[102] "The Internet in Britain: 2007," p. 8.
[103] "The Communications Market: Broadband Digital Progress Report," p. 2.
[104] "The Communications Market: Broadband Digital Progress Report," p. 3.
[105] "The Communications Market: Broadband Digital Progress Report," p. 3.
[106] "The Communications Market: Broadband Digital Progress Report," p. 21.

Internet Safety Initiatives

Government-led Initiatives

From the initial stages of the Internet, the government has been central in helping to ensure that the Internet is made as safe as possible for everyone, children in particular. This began with work on the IWF and the ITFCPI, and continues through to the present, with the Prime Minister recently announcing a government consultation on the effects of the media, including the Internet, on children. Some of the initiatives that have been led by the UK government are outlined below:

The Internet Task Force for Child Protection on the Internet (ITFCPI)

ITFCPI was established in March 2001 in response to a report by the Internet Crime Forum. Its objective is to make the UK the best and safest place in the world for children to use the Internet, and to help protect children the world over from abuse fuelled by criminal misuse of new technologies.[107] It has produced a range of guidance notes including:

- **Good Practice Guidance for the Moderation of Interactive Services for Children**[108] - This guidance note provides information and recommendations for the moderation of public interactive communication services, which are intended for or are very likely to attract children, in relation to information and advice to users, risk assessment, recruitment, training, data security, management and supervision, and escalation procedures.
- **Good Practice Guidance for Search Service Providers and Advice to the Public on how to Search Safely**[109] - This document is aimed at the public, as well as at companies who provide search tools across all platforms, whether via personal computer, mobile phone or any other means.
- **Promoting Internet Safety through Public Awareness Campaigns Guidance for Using Real Life Examples Involving Children or Young People**[110] - This document offers guidance for using real life examples involving children or young people in Internet safety public awareness campaigns.
- **Good Practice Models and Guidance for the Internet Industry on: Chat Services, Instant Messaging, and Web-based Services**[111] - This guidance note introduces a variety of models of good practice for the

[107] http://police.homeoffice.gov.uk/operational-policing/crime-disorder/child-protection-taskforce
[108] http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/moderation-document-final.pdf
[109] http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/search-and-advice-public.pdf
[110] http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/RealLifeExamples.pdf
[111] http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/ho_model.pdf

provision of different kinds of Internet services by a range of companies and organizations that are active in the online world.

Child Exploitation and Online Protection (CEOP) Centre

A government agency launched in April 2006, the CEOP Centre[112] works across the UK and with organizations around the globe to deliver a new approach that combines police powers with the dedicated expertise of industry, government, specialist charities and other related organizations that are all focused on tackling child sex abuse wherever and whenever it happens. Some of CEOP's initiatives are as follows:

- **Think U Know** - This initiative is aimed at educating children and parents about safe surfing via a website[113] containing information on Internet safety. The site covers a range of topics, including social networking, mobiles, blogging, and gaming sites. It also allows visitors to quickly and easily make a report if they feel uncomfortable or worried about someone they are chatting to online.

BECTA

BECTA[114] is the government's education technology agency, which provides advice and support on a wide range of Internet-related issues of interest to schools, from finding an Internet service provider and getting the school connected to ensuring the safety of students when they use the Internet. To ensure students' safety, BECTA gives advice on setting an Internet use policy in order to reduce risks online and provides free of charge a brochure entitled "Safeguarding children online: a guide for local authorities and local safeguarding children boards."[115]

Scottish Qualifications Authority (SQA)[116] Internet Safety Qualification[117]

A Scottish initiative that was launched in August 2006 in conjunction with Stathclyde Police, the SQA provides a unique qualification for children, parents and the elderly, and is the only nationally recognized training course of its kind.

[112] http://www.ceop.gov.uk/
[113] http://www.thinkuknow.co.uk/
[114] BECTA stands for the British Education Communication Technology Agency, but the full name of the agency is rarely used. For information on the agency, see: http://www.becta.org.uk/.
[115] http://publications.becta.org.uk/display.cfm?resID=31049&CFID=1300168&CFTOKEN=83c4d7bb90d0a9f-6FFF43BB-E989-9175-B09ADEC59D711549
[116] The Scottish Qualifications Authority is an executive non-departmental public body (NDPB) sponsored by the Scottish Executive Education Department. See: http://www.sqa.org.uk/sqa/CCC_FirstPage.jsp.
[117] FAQs and other information on the Internet Safety Qualification can be found at: http://www.sqa.org.uk/sqa/25333.html

The course, which is delivered predominantly by email and has two quizzes, covers topics such as: dealing with junk mail, identity theft, protecting systems against viruses, theft, grooming, and phishing and pharming.

Changes in the Law

The passing of the "S.46 Sexual Offences Act 2003"[118] made an amendment to the "Protection of Children Act 1978"[119], prohibiting the "taking or making" of indecent photographs or pseudo-photographs of a child. However in the case that IT personnel need to make such a photograph for the purpose of prevention, detection, or investigation of a crime or for criminal proceedings, this is allowed. Also, a person accidentally finding such an image has a defence against making.

Charity Initiatives

Some UK children's charities, Barnardos[120]; Childline[121]; ECPAT[122]; National Children's Bureau[123]; NCH (the Children's Charity)[124]; the National Council of Voluntary Child Care Organizations (NCVCCO)[125]; the National Society for Prevention of Cruelty to Children (NSPCC)[126]; Stop it Now! UK & Ireland[127]; and The Children's Society[128], have come together to form the Children's Charities' Coalition for Internet Safety (CHIS)[129]. This united organization brings together all of the expertise from each of the charities to develop initiatives and work closely with industry organizations, law enforcement agencies and the government. Some of CHIS' members' individual initiatives are:

Internet Watch Foundation (IWF)

Internet Watch Foundation (IWF)[130] is a charity founded as the result of an agreement between the government, police and the Internet industry, and is the only authorised 'hotline' in the UK for the members of the public to report their inadvertent exposure to illegal content on the Internet. It has worked on a range of initiatives since its formation in 1996, including the INFORM Campaign for UK

[118] http://www.opsi.gov.uk/acts/acts2003/20030042.htm
[119] http://www.opsi.gov.uk/acts/acts1978/PDF/ukpga_19780037_en.pdf
[120] http://www.barnardos.org.uk/
[121] http://www.childline.org.uk/
[122] ECPAT stands for "End Child Prostitution, Child Pornography and the Trafficking of Children for Sexual Purposes". Information on this organization can be accessed at: http://www.ecpat.org.uk/.
[123] http://www.ncb.org.uk/Page.asp
[124] http://www.nch.org.uk/
[125] http://www.ncvcco.org/
[126] http://www.nspcc.org.uk/
[127] http://www.stopitnow.org.uk
[128] http://www.childrenssociety.org.uk/
[129] http://www.nch.org.uk/information/index.php?i=210
[130] http://www.iwf.org.uk/

Police[131]. This is a partnership between the IWF and the Association of Chief Police Officers (ACPO)[132] to raise awareness of the IWF and its activities and initiatives, and to inform police officers and their staff when the public should be referred to the IWF.

Stop it Now! UK & Ireland

Stop it Now! UK & Ireland[133] is a campaign, run under the auspices of the Lucy Faithfull Foundation,[134] aimed at preventing child sexual abuse by increasing public awareness and empowering all adults to act responsibly to protect children. Part of its program is a guide, entitled "The Internet and Children - What's the Problem?"[135], which moves away from the traditional approach of talking about risks new technologies pose to children's safety. Instead, it is a no-nonsense guide that details the tell-tale signs to look for in children if they are a victim of online sexual abuse or if they suspect a friend, colleague or relative may be using technologies in an inappropriate or harmful way.

NCH (the Children's Charity)

NCH[136] has run a series of campaigns for wider access to information and communication technology for children from less advantaged backgrounds. It also strongly promotes online safety for all children and has launched a Net Smart programme.[137]

Industry-led Education Initiatives

Industry has been at the heart of the majority of Internet safety initiatives, with companies contributing in a wide variety of ways to help support online safety activities. They also work on initiatives themselves to help drive awareness and protect Internet users. Some of these are:

Get Safe Online

This was a joint industry, police and government initiative to highlight the threats people face online and what they can do to combat them. It included a high-profile campaign to drive awareness and a website[138] from which a series of easy-to-understand guides on common threats could be downloaded.

[131] http://www.iwf.org.uk/media/page.158.htm
[132] http://www.acpo.police.uk/
[133] http://www.stopitnow.org.uk
[134] http://www.lucyfaithfull.org/
[135] http://www.stopitnow.org.uk/Green%20Book.pdf
[136] http://www.nch.org.uk/
[137] http://www.nch.org.uk/information/index.php?i=209
[138] http://www.getsafeonline.org/

BT Cleanfeed

Cleanfeed[139] is an advanced filtering technology that prevents BT's Internet customers from accessing content that is illegal under UK law and on the IWF's URL blacklist. The system blocks tens of thousands attempts to access illegal content each day. BT is also sharing the technology with other ISPs across the world for free, so they can offer similar levels of protection to customers.

Internet Green Cross Code

The Internet Green Cross Code[140] was the first educational initiative aimed at teaching children about the dangers associated with the Internet. It was developed by BT and supported by HM Home Office, police and some children's charities.

AOL UK - www.aol.co.uk
BECTA - www.schools.becta.org.uk
BT - www.bt.com
Chat Danger - www.chatdanger.com
Child Exploitation and Online Protection (CEOP) Centre - www.ceop.gov.uk
Childnet International - www.childnet-int.com
Crisp Thinking - www.crisp.com
Department for Education and Skills (DfES) - www.safety.ngfl.gov.uk/schools/
Get Safe Online - www.getsafeonline.org
HM Home Office - www.homeoffice.gov.uk
Internet Watch Foundation - www.iwf.org.uk
Kidsmart - www.kidsmart.org.uk
NCH (the Children's Charity) - www.nch.org.uk
National Society for Prevention of Cruelty to Children (NSPCC) - www.nspcc.org.uk
Ofcom - www.ofcom.org.uk
Serious Organised Crime Agency (SOCA) - www.soca.gov.uk
Stop it Now! UK and Ireland - www.stopitnow.org.uk
Think U Know - www.thinkuknow.co.uk
Virtual Global Taskforce - www.virtualglobaltaskforce.com

Conclusion

There is currently no single solution for keeping children safe online; however technology, education, regulation and self-regulation all have roles to play.

The dilemma we face is ever-changing due to the speed at which Internet technology is developing. Once our worries were predominantly about children accessing or downloading adult content, but now the greater issue is that

[139] http://www.cleanfeed.co.uk/
[140] http://www.bteducation.org/resources/view.ikml?id=80

children can upload information about themselves and others; a problem no one would have predicted five years ago. We are currently reading headlines about social networking sites and the risks they pose, but these are only the tip of a very large iceberg. The widespread use of mobile phones, webcams and digital cameras to capture and publish intimate details of children's lives online is an emerging problem.

It is simply not feasible to review all content that is uploaded onto the Internet, so education, both for children and the adults who look after them, is essential. However, we do not yet have a consistent message that is easily understood and translated universally, like the 'Smoking Kills' health warnings on tobacco products. It may sound defeatist to suggest that there is no silver bullet[141] to make the Internet a safe place for children, but exactly the same could be said of the offline world. The critical thing now for governments, law enforcement agencies and industry, as well as for parents, guardians and teachers is to work together and find the right balance of caution and warnings while allowing children the freedom to discover for themselves what the Internet has to offer.

[141] No silver bullet means that there is no instant remedy. The term comes from folklore - the silver bullet was the only kind of bullet that could kill a werewolf, witch, vampire, or monster. For more information on the etymology, see: http://www.wisegeek.com/what-is-a-silver-bullet.htm.

Chapter III:
Germany

by Thomas Rickert
Director of Self-Regulation, eco - Verband der Deutschen Internetwirtschaft
(Federation of the German Internet Economy) e.V, Germany

Existing Legislation in Germany Regarding Online Safety and Technology Solutions Offered by Companies

In April 2003, new legislation on youth protection, the Youth Protection Act (Jugendschutzgesetz - JuSchG)[142] and the Interstate Treaty for the Projection of Human Dignity and the Protection of Minors in the Media (Jugendmedienschutz-Staatsvertrag - JMStV)[143], entered into force. These laws provide for a unified legal response to the challenges of an increasingly convergent world, and are meant to complement the existing provisions on youth protection in the Federal Criminal Code.

Before the new legislation was introduced, there were difficulties for both the industry and the competent authorities resulting from the federal system in Germany. While broadcasting is a matter that the German Federal States (Länder) are responsible for, the Federal Government is competent for technology. As a consequence, an array of authorities was competent for the relevant subject matter.

As a component of the new legislation, the Commission for the Protection of Minors in the Media (Kommission für Jugendmedienschutz - KJM)[144] was founded to be the body responsible for youth protection in commercial broadcasting services and telemedia. Under the terms of the JMStV, the Commission evaluates television and Internet services for the whole country and the JuSchG monitors products distributed via a storage media, such as videotapes, DVDs and CDs.

As the focus of this chapter is on the online world, from hereon in only the provisions of the JMStV will be discussed. In particular, the new concept of so-called “regulated self-regulation”[145], which was introduced in the JMStV, will be examined.

---

[142] A summary in German can be found at:
http://www.bmfsfj.de/Kategorien/gesetze,did=5350.html and an English version of the law (in its entirety) can be obtained at:
http://www.bmfsfj.de/bmfsfj/generator/RedaktionBMFSFJ/Abteilung5/Pdf-Anlagen/juSchGenglisch,property=pdf,bereich=,sprache=de,rwb=true.pdf

[143] http://www.artikel5.de/gesetze/jmstv.html

[144] http://www.kjm-online.de/public/kjm/

[145] Information on this concept and the requirements for self-regulatory bodies are available in English at: http://www.fsf.de/fsf2/international/summary.htm.

This idea means that the JMStV makes it possible to allow self-regulatory bodies to make independent decisions on complaints, within clearly defined boundaries, for content or service providers that affiliate with the self-regulatory body and who subscribe to its complaints procedure. However, these self-regulatory bodies need to be accredited with KJM and fulfil the following criteria:

- The independence and expertise of the examiners needs to be assured.
- An appropriate scheme needs to be ensured by a multitude of providers (for financial viability).
- Guidelines for the examiners, which provide for effective protection of children and young people when decisions are made, are needed.
- A complaints procedure detailing the scope of the examination, and in the case of broadcasting an obligation to have content pre-checked as well as a possibility to appeal the decisions, is required.
- The provider in question must have his voice heard before a decision is taken and the grounds for the decision must be laid down in writing and communicated to all the relevant parties.
- A complaints office needs to be in operation.

Participating service providers benefit from legal privileges, unless the self-regulatory body has gone beyond its power for decision-making.

Since November 2004, the Association for the Voluntary Self-Monitoring of Multimedia Service Providers (Freiwillige Selbstkontrolle Multimedia-Diensteanbieter - FSM)[146] has been accredited by KJM to act as the self-regulatory body for online services. Its initial appointment was subject to conditions; however these have all been fulfilled subsequently.

Under the new law, a distinction is made between three categories of content: strictly prohibited content; minor forms of prohibited content; and content detrimental to the development of children and young people (harmful content).

According to section 4.1 of the JMStV it is strictly prohibited to present online content such as:

- child pornography;
- bestiality;
- Nazi propaganda;
- incitement to racial hatred;
- Holocaust denial;

[146] www.fsm.de/en/

- certain depictions of cruelty or glorification of violence against human beings (which is also applicable for virtual depictions);
- glorification of war;
- depictions of people suffering in a manner that violates their human dignity; and
- depictions of children and young people in an unnatural sexual pose (also applicable to virtual depictions).[147]

In addition to these provisions of the JMStV, making above content can be punishable under the Criminal Code.

According to section 4.2 of the JMStV it is also prohibited to publish content, such as: simple pornography (which does not fall under the provisions under section 4.1) and other types of content which may cause serious harm to minors.[148] While such content must not be made available via broadcasting services, there is an exception for Internet content. Such content may be legally published online if the content provider ensures that it can only be accessed by adults.

In order to ensure that simple pornography and other harmful content are not accessed by children, KJM has developed criteria for age verification systems to establish closed user groups. The KJM age verification systems involve two steps, identification and authentication. A face-to-face control or other technical method is required to verify that the person is an adult in the first phase, then the user needs to authenticate him/herself anytime the service is used to avoid his/her access data being passed on to third parties. This can be achieved by using PIN numbers.

KJM evaluates age verification systems upon request and as of October 2007 has confirmed that 18 systems are compliant with the requirements of the JMStV. However, recently there has been heated debate as to whether KJM is entitled to carry out evaluations because the JMStV does not stipulate that KJM has the authority to accredit age verification systems.[149] The Bundesgerichtshof, the highest appeals court in Germany, recently ruled that an identity card number check is insufficient, even if an additional postal code check or money transfer is required (I ZR 102/05).[150]

According to JMStV section 5.1, content that might impair the development of minors must only be distributed or made available in a manner that young people

[147] http://www.artikel5.de/gesetze/jmstv.html#p4 (available in German only)
[148] http://www.artikel5.de/gesetze/jmstv.html#p4
[149] Competences of the KJM are outlined in Section 16 of the JMStV available in German at: http://www.artikel5.de/gesetze/jmstv.html#p16.
[150] The court made this ruling on October 18, 2007. A press release about it can be found in German at: http://www.heise.de/newsticker/meldung/97651

usually cannot access it. This can be achieved by: technical or other means (section 5.3.1) or limitations of broadcasting time (section 5.3.2).[151]

With regard to the use of technical means, it shall be noted that in contrast to pornographic content, where an age verification system must *ensure* that only adults can access the material, in this case the content provider *only* needs to take measures that would *usually* prevent access by minors to harmful content.

One possibility for a content provider to fulfil this legal requirement is to use a youth protection program, accredited by KJM, according to section 11[152] of the JMStV. In other words, the content provider cannot just use any filtering software available in order to be compliant and legally privileged. However, to date, no youth protection program has been accredited by KJM. On the contrary, KJM has publicly stated that no system currently available would fulfil their requirements.

However, the JMStV allows for test phases to evaluate new technical approaches. One test phase has been carried out by an industry consortium led by eco, but it has not received KJM accreditation. Yet, the industry consortium is still working with KJM to further define criteria for a youth protection program that would qualify for accreditation.

One of the primary reasons for the difficulties with attaining accredited status is that the JMStV does not make explicit any requirements apart from access to contents must be different for different age groups and content providers must have the possibility to program contents for a youth protection program.

KJM, on the other hand, requires a modular system, which consists of a filtering unit, a block list, an allow list, and a possibility to program contents for the filtering system. With respect to the last requirement, KJM has stated that every youth protection program seeking accreditation needs to be capable of reading ICRA labels, which are widely regarded as a successful way to encode contents. In fact, the industry consortium has proposed an approach including ICRA and eco has been promoting ICRA for many years and has been the German point of presence since 2003.[153]

As a consequence of the lack of accredited youth protection programs, only the second option of section 5.3.2 of the JMStV (introduced above), the limitation of broadcasting time, can be used effectively by content providers to be compliant. While this might seem to be an anachronistic measure for Internet services, many portals actually look different during the day than during the night time, which is a consequence of the legal requirements.

[151] http://www.artikel5.de/gesetze/jmstv.html#p5
[152] http://www.artikel5.de/gesetze/jmstv.html#p11
[153] Press releases detailing eco's role as ICRA's point of presence in Germany can be found in English at: http://www.fosi.org/press/en_icradeutschland/ and in German at: http://www.eco.de/arbeitskreise/2397.htm.

Whereas KJM has reiterated in a press release of October 29, 2007 that available filtering systems are not efficient enough based on tests carried out by jugendschutz.net, the results of a test carried out by the reputable c't computer magazine[154] have been much more favorable.

While it is KJM's point of view that the best possible protection level for underage users should be provided, it can only be hoped that progress will be made quickly in providing users with an accredited youth protection program since the new law was introduced more than four years ago. Questions are being asked by interested parties whether one should wait for a "perfect system" or if it is better to make one of the existing products available to users and industry as an accredited system now.

It should be noted that many service providers offer their customers filtering tools, which are suitable for protecting young people, but which have not been accredited by KJM. Part of the reason why these companies have not applied for accreditation is that they fear that KJM could reject the application and that would in turn cause bad publicity.

The new regulation is currently under evaluation and a vivid debate on what changes need to be made in order to improve the system is underway. The Hans-Bredow Institute for Media Research at Hamburg University has been commissioned to prepare this evaluation scientifically. The comprehensive study is available in German at http://www.hans-bredow-institut.de/.

Educational Efforts by Government, Charities, Schools, Local Councils, and Companies

There are numerous initiatives being carried out to respond to the negative issues on the Internet in Germany. The following list of actions and initiatives is not comprehensive.

Deutschland Sicher im Netz

"Deutschland sicher im Netz" (Germany Securely on the Net - DSIN)[155] is the largest safety initiative in Germany. DSIN is a coalition of several large enterprises and associations, including eco, of the Internet industry. The aim of the initiative is to give the general public tools and information so they can use the Internet in a safe and secure way.

On June 19, 2007, a collaboration agreement between DSIN and the German Federal Ministry of Interior was signed, making Federal Minister, Dr. Wolfgang

[154] c't stands for Computer Technology. Information on this magazine can be found in German at: http://www.heise.de/ct/ and in English at: http://www.heise.de/ct/english/.
[155] www.sicher-im-netz.de

Schäuble, the patron of the association which has since become the official private partner of the Ministry in Internet security matters.[156]

eco - Verband der Deutschen Internetwirtschaft e.V. (Federation of the German Internet Economy)

eco[157] is an Internet Service Providers Association which was founded in 1995. As a body, eco sees itself as the advocate and mouthpiece of German Internet business in the relevant political, legislative and international groupings. In addition to operating a hotline together with FSM (which will be described in more detail later in this article), eco has for many years been promoting the ICRA content labeling scheme to industry, users and public authorities. eco is currently chairing an industry consortium that promotes content filtering based on the ICRA approach. Additionally, eco is advising its members, as well as the general public, on countermeasures to the dangers of the Internet and on how to best respond to illegal and harmful material online. This initiative consists of information on the website, seminars and brochures. eco is a founding member of FSM and INHOPE.

Ein Netz für Kinder (A Net for Children)[158]

In 2007, the Federal Government Commissioner for Culture and the Media, Bernd Neumann, launched an initiative called “Ein Netz für Kinder” as a public-private partnership of political and legal institutions and industry to set up a safe environment for children to surf. This initiative aims to establish a list of websites that are suitable for children and young people, as well as to stimulate the creation of suitable high quality contents by means of a federal funding program.

FSM - *Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e. V.* (Association for the Voluntary Self-Monitoring of Multimedia Service Providers)

FSM[159] is the German association for voluntary self-regulation in online media, which has been accredited by KJM. The purpose of this association is to promote self-regulation, education and training in the multimedia area. FSM provides information for both multimedia service providers and users of the Internet on the legal framework of online media, online filter technology, content rating, and other related matters. FSM operates the Internet Complaints Office (Internet Beschwerdestelle) website[160] together with eco and is a founding member of

[156] http://www.bmi.bund.de/nn_163922/Internet/Content/Nachrichten/Pressemitteilungen/2007/06/Deutschland__sicher__imNetz.html
[157] http://www.eco.de/
[158] http://www.media.nrw.de/media2/site/index.php?id=73&tx_ttnews%5Btt_news%5D=52189&cHash=1c37744179
[159] Information in English can be accessed at: http://www.fsm.de/en/, while the German page is available at: http://www.fsm.de/.
[160] www.internet-beschwerdestelle.de/

INHOPE. In addition, FSM is managing the “Ein Netz für Kinder” project and co-operating the educational website www.internauten.de.

Internet-Beschwerdestelle.de

Jointly operated by eco and FSM, the Internet Complaints Office (Internet-Beschwerdestelle)[161] is an Internet hotline that takes complaints from the public about illegal and harmful Internet content.

Both eco and FSM are founding members of the INHOPE Association[162], the umbrella organisation of Internet hotlines which now has 30 members from 27 countries worldwide to respond to illegal content, in particular child pornography. The internet-beschwerdestelle.de website has been set up as a one stop shop for Internet safety as it contains links to relevant organizations, as well as educational materials for downloading. The Internet Complaints Office is financially supported under the European Commission’s Safer Internet Program.

Jugendschutz.net

Jugendschutz.net was established by the ministers of youth of the German Federal States. Since a change in the German legislation in 2003, jugendschutz.net is organizationally attached to the KJM.

Since 2000, jugendschutz.net has been operating a hotline (which is part of the INHOPE network) to which Internet users can report content they deem to be illegal. In addition to the hotline work, jugendschutz.net is carrying out research, particularly in the areas of right-wing extremism, Internet chatting and other areas relevant to protection of youth online. Educational information is made available on the website, in brochures and reports.

Klicksafe.de

Klicksafe.de[163] is the German awareness node co-financed by the European Commission’s Safer Internet Program and part of the Insafe Network[164], the European network of e-safety awareness nodes. The project partners Landeszentrale für Medien und Kommunikation (LMK) Rheinland-Pfalz (Center for Media and Communication for the Rheinland-Pfalz Region), Landesanstalt für Medien (LfM) Nordrhein-Westfalen (Institute for Media for the Nordrhein-Westfalen Region) and the European Center for Media Competence (ecmc) are working together to raise public awareness on the topic of Internet safety. In addition to providing the klicksafe.de portal, the consortium seeks to improve the

[161] www.internet-beschwerdestelle.de
[162] www.inhope.org
[163] The English version of this site can be found at: http://klicksafe.de/common/english.php and the German one is available at: http://klicksafe.de/.
[164] www.saferinternet.org

protection level of minors by creating youth-focused TV clips, directly approaching the target groups in question, training educators, and carrying out regional and national topical events.

National Integration Plan

This program[165], presented by Chancellor Angela Merkel in July 2007, which promotes the competent and efficient use of media by migrants, is seen as a prerequisite to successful integration. One of the main measures of the plan is to provide educational material in other languages than German and to foster media literacy amongst migrants. The klicksafe consortium has committed itself to helping achieve the goals of the National Integration Plan by getting new immigrants informed and improving their awareness of the risks involved in using online services.

Conclusion

There are numerous initiatives in Germany to make the Internet a safer place to be for children and young people. Some of these initiatives have been started many years before the new legal system has been introduced. While the general approach to harmonise youth protection in all media in a federal system is welcome, some aspects of the system have shown to be in need of improvement. An evaluation of the law is currently being carried out and some of the weaknesses of the concept are hopefully going to be altered for the better in order to make the system work more effective in practice.

[165] A flyer outlining the National Integration Plan in English can be found at: http://www.bundesregierung.de/Content/DE/Publikation/IB/Anlagen/ib-flyer-nip-englisch-barrierefrei,property=publicationFile.pdf

Chapter IV:
Australia

by Australian Communications and Media Authority
Sydney, Australia

Overview

This chapter provides an overview of the use of online and mobile technologies in Australia and the way by which the Australian Government has addressed community concerns about the safety issues posed by online and mobile telephone content.

Section 1 of this chapter contains information about Internet use and mobile telephone penetration in Australia, as well as studies of children's Internet habits and the uptake of Internet content filters in Australia.

Section 2 outlines Australia's legislative and regulatory environment in the area of online safety, including recent developments which have extended the regulatory framework to encompass new types of content services.

Section 3 details community education and awareness initiatives, including the recently launched *NetAlert – Protecting Australian Families Online* (PAFO) project. Informed by research, these initiatives provide users with the tools and information to manage access to the Internet for themselves and their children.

Section 4 provides information about Internet content filter technology available in Australia as well as developments in this area.

1: Basic Statistics: Internet Use, Filters and Mobiles

Internet Use

At the end of March 2007, Australia had 6.43 million active Internet subscribers comprising 5.67 million households, 67 percent of which subscribed to a broadband service (defined as a service providing download speeds of at least 256 kbit/s).[166]

In December 2006, the Organization for Economic Co-operation and Development (OECD) estimated Australia's total broadband subscribers at

[166] Australian Bureau of Statistics, *8153.0 Internet Activity, Australia, Mar 2007*, http://www.abs.gov.au/ausstats/abs@.nsf/mf/8153.0/ (Internet Activity, March 2007).

3,939,288, equating to a penetration rate of 19.2 subscribers per 100 inhabitants (compared with an OECD average of 16.9). The penetration rate has increased significantly from 7.7 subscribers per 100 inhabitants in 2004 and 13.8 subscribers per 100 inhabitants in 2005.[167]

Digital subscriber line continues to be the dominant access technology, used by 78 percent of broadband subscribers in 2007.[168] Broadband take-up has increased by between 90 and100 percent each year from 2002 to 2005. There was a lower rate of growth of 51 percent between 2005 and 2006; however this was expected due to the larger base number of broadband connections.[169]

According to the *kidsonline@home: Internet use in Australian homes* report,[170] which was prepared for the Australian Broadcasting Authority and NetAlert Limited in 2005,[171] children are increasingly accessing the Internet at a younger age. Just over a third of 8 and 9 year olds had started using the Internet at age 5 or 6. Of children aged 12 and 13 years, 25 percent first accessed the internet at age 9 or 10.[172]

37 percent of Australian children accessed the Internet on a daily basis and a further third accessed it two to three times a week. This is an increase from previous years - in 2001, only 5 percent of 11 and 12 year olds, and one-third of 13 and 14 year olds were online daily, but remained on less frequently than children in Hong Kong and the United Kingdom.[173]

The report found that frequent Internet use was more common among children accessing the Internet via a broadband connection.[174] To help gauge the extent to which children's internet use is supervised in the home, parents were asked which room the computer connected to the internet is located in. The most common location for Internet access by children 8 to 13 years old was the study (48 percent), followed by the lounge or family room (25 percent).[175]

---

[167] Organisation for Economic Co-operation and Development, *OECD Broadband Statistics to December 2006*, http://www.oecd.org/document/7/0,3343,en_2649_34225_38446855_1_1_1_1,00.html.

[168] Internet Activity, March 2007.

[169] Australian Competition and Consumer Commission, *Snapshot of Broadband Deployment as at 30 September 2006*, http://www.accc.gov.au/content/item.phtml?itemId=781269&nodeId=aac2cffa7bd9177dbdedb20ac5a9d601&fn=Snapshot%20of%20broadband%20deployment%20(30%20Sep%2006).pdf.

[170] NetRatings Australia Pty Ltd for the Australian Broadcasting Authority and NetAlert Limited, *kidsonline@home: Internet use in Australian homes*, http://www.acma.gov.au/webwr/_assets/main/lib100852/kidsonline.pdf (kidsonline@home).

[171] On July 1, 2005, the Australian Broadcasting Authority and the Australian Communications Authority merged to form the Australian Communications and Media Authority (ACMA). In 2007 NetAlert Limited merged with ACMA.

[172] kidsonline@home, 19.

[173] kidsonline@home, x.

[174] kidsonline@home, 16.

[175] kidsonline@home, 17.

The most popular use of the Internet by children at home was for homework or study (88 percent of children), followed by games (80 percent), email (64 percent), and instant messaging (40 percent). Fewer children used the Internet to download music (26 percent) or chat (18 percent).[176] Boys and younger children were more likely to access the Internet for entertainment (games, websites and music), while girls and older children were more likely to use it as a communication resource (email and instant messaging).[177]

Additionally, the Australian Bureau of Statistics (ABS) has conducted a series of surveys into children's participation in cultural and leisure activities, including time spent accessing the Internet. Surveys were conducted in April 2000, 2003, and 2006. The 2006 survey identified that for the 12 months prior to April 2006, 65 percent of Australian children aged 5 to 14 years (1.73 million children) accessed the Internet.[178] Although not unexpected, this was a notable increase since April 2000, when 47 percent of children accessed the Internet.[179]

The survey found that the frequency of Internet access also increased with age: 10 percent of 5 to 8 year olds were found to access the Internet daily, compared with 18 percent of 9 to 12 year olds and 39 percent of 12 to 14 year olds.[180]

Children who accessed the Internet most commonly did so at home (85 percent or 1.47 million) or at school (75 percent or 1.29 million).[181] These two locations have remained the most popular points of access for children since the original survey in 2000, at which time access at school (67 percent) was slightly more common than access at home (56 percent).[182]

In 2007, the Australian Communications and Media Authority (ACMA) completed research about the use of media and communications devices in Australian families. The research was comprised of two main components - a survey of 750 families, and completion of media usage diaries by 1000 families. A literature review on the influence of electronic media and communications devices on children and families was also undertaken as part of this project.[183]

---

[176] kidsonline@home, 24.
[177] kidsonline@home, 25.
[178] Australian Bureau of Statistics, *4901.0 - Children's Participation in Cultural and Leisure Activities, Australia, Apr 2006*, http://www.abs.gov.au/Ausstats/abs@.nsf/Lookup/0B14D86E14A1215ECA2569D70080031C (Children's participation, April 2006).
[179] Australian Bureau of Statistics, *4901.0 Children's Participation in Cultural and Leisure Activities, Australia April 2000*, http://www.abs.gov.au/AUSSTATS/abs@.nsf/allprimarymainfeatures/2396F6D4AA80BB49CA256E2A00765A06?opendocument (Children's participation, April 2000).
[180] Children's participation, April 2006.
[181] Children's participation, April 2006.
[182] Children's participation, April 2000.
[183] A description of the research objectives is included in the Request for Expressions of Interest for undertaking the Media and Society review of research literature, which can be found at:

The final report was delivered to the Department of Communications, Information Technology and the Arts (DCITA) at the end of August 2007, and ACMA will publish the final report in a forthcoming publication.

Uptake of filters

The *kidsonline@home: Internet use in Australian homes* report also included a survey about the use of Internet content filters by Australian families. The report found that 35 percent of parents surveyed used software to filter inappropriate websites. Twenty-nine percent of parents surveyed used filters on a regular basis and 6 percent used them occasionally. Fifty-six percent of parents surveyed did not use filters, 4 percent used filters at one point, but no longer did, and 5 percent were not sure whether they used filters.

Of parents who chose not to use filter products, 17 percent felt that installing filter software was redundant as other safeguards were in use, with parents of younger children (8 or 9 years old) most likely to cite this as the reason. Five percent of parents said they did not use a filter because they were 'unsure how to install' one, 4 percent were 'unsure of its use', and 3 percent were 'unsure of where to obtain a filter'. A small proportion (4 percent) cited filters as being too restrictive. Half of all households surveyed who did not use filter products noted that they felt trust of their child was sufficient to 'protect them from all of the safety issues that the Internet raises'.[184]

In August 2007, the Government announced the *NetAlert – Protecting Australian Families Online* initiative (detailed in Section 3). The initiative includes a scheme to make a free Internet content filter available to every Australian household. It is expected that the initiative will substantially increase the use of filters in Australian households.

Uptake of mobile phones

Data provided to ACMA by the telecommunication industry showed that mobile telephone penetration in the Australian market grew by 7 percent in 2005–2006 to 19.7 million services.[185] The majority of users access a GSM mobile network, which provides coverage to 96 percent of the Australian population.[186]

Australia's mobile phone carriers began launching 3G mobile networks in late 2005. Since that time, 3G mobile services have undergone significant growth

---

http://www.acma.gov.au/webwr/_assets/main/lib100880/eoi%2006-acma007.pdf.

[184] kidsonline@home.

[185] Australian Communications and Media Authority, *Communications Infrastructure and Services Availability in Australia 2006-07*, http://www.acma.gov.au/WEB/STANDARD/pc=PC_100215.

[186] Australian Communications and Media Authority, *Communications Infrastructure and Services Availability in Australia 2006-07*, http://www.acma.gov.au/WEB/STANDARD/pc=PC_100215.

with the number of users reaching 1.6 million in June 2006.[187] At the time of writing, all four major Australian mobile carriers (Telstra, Optus, Vodafone and Hutchison) are developing plans to roll out next generation networks, capable of providing data transfer speeds of up to 14.4 mbit/s.

2: Legislation and Regulatory Structures

Internet Content Regulation

Australia's Online Content Co-regulatory Scheme (the online content scheme) evolved from a tradition of content regulation in broadcasting and other entertainment media.

A national approach to the classification of cinema films and related home-based formats was settled in 1984, based on the principle that, while adults should be free to see, hear and read what they want, children should be protected from material that may be unsuitable for or harmful to them, and everyone should be protected from unsolicited material that is highly offensive. In 1995, the *National Classification Code* formalized the current framework of classifications and consumer advice, which now applies across most audio-visual platforms.[188] This framework is generally well understood by the community and industry.

The Online Content Co-regulatory Scheme

ACMA has administered the online content scheme since January 2000. Set out under Schedule 5 of the *Broadcasting Services Act 1992* (the Act), the scheme seeks to protect children from exposure to unsuitable Internet content and to restrict access to certain Internet content that is likely to cause offense to adults. The scheme seeks to achieve these objectives by a number of means, including:

- coordinating community education activities targeted primarily at children;
- establishing links between Government and industry; and
- providing a process for the public to have complaints about offensive or illegal Internet content addressed.

As the body charged with administering the scheme, ACMA's responsibilities include:

- investigating complaints about Internet content, and taking action in relation to content that is prohibited under the Act;

[187] Australian Communications and Media Authority, *Communications Infrastructure and Services Availability in Australia 2006-07*, http://www.acma.gov.au/WEB/STANDARD/pc=PC_100215.

[188] Prior to the introduction of the *National Classification Code*, Commonwealth and State governments administered separate classification schemes. The *National Classification Code* is set out in the *Classification (Publications, Films and Computer Games) Act 1995*, http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/current/bytitle/7655DE6FA2B304CCCA257355001C8821?OpenDocument&mostrecent=1.

- encouraging development of codes of practice for the Internet industry, and registering, monitoring compliance with, and enforcing such codes;
- providing advice and information to the community about Internet safety issues, especially those relating to children's use of the Internet (discussed in Section 3); and
- undertaking activities including research and international liaison.

While the administration of the online content scheme is the responsibility of ACMA, the principle of co-regulation embodied in the scheme reflects Parliament's intention that government, industry and the community all play a role in managing Internet safety issues in Australia, particularly Internet safety for children.

Complaints Handling

A central feature of the online content scheme is the mechanism that allows members of the Australian public to submit complaints to ACMA about Internet content that is, or may be, prohibited by law. The use of a complaints-based regulatory mechanism was considered important to avoid unnecessary financial and administrative burdens on industry because it is a reactive system which does not require Internet service providers (ISPs) and Internet content hosts (ICHs) to actively review, monitor or engage in universal blocking of content.

Under Schedule 5 of the Act, ACMA must investigate legitimate complaints about potentially prohibited Internet content. According to the Act, Internet content is stored information that is accessed over an Internet carriage service, including: material on the World Wide Web, postings on newsgroups and bulletin boards, and files that can be downloaded via file transfer protocol (FTP) sites and peer-to-peer networks. Currently, for the purposes of the scheme, Internet content does not include ordinary email (including spam)[189] or information that is accessed in real time without being previously stored, such as chat services and voice over the Internet (VoIP).[190]

In assessing whether or not Internet content is, or may be, prohibited, the content is classified according to the *National Classification Code* (the Code)[191] and the

[189] However, ACMA does investigate complaints about spam emails under a separate legislative scheme established by the *Spam Act 2003*. For further information see: http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/current/bytitle/E9920A4E670D0FC8CA25702600124DC5?OpenDocument&mostrecent=1.

[190] Schedule 5, *Broadcasting Services Act 1992*, http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/current/bytitle/B15DD32964880061CA2573250006F81F?OpenDocument&mostrecent=1.

[191] http://www.comlaw.gov.au/comlaw/management.nsf/lookupindexpagesbyid/IP200508203?OpenDocument.

Guidelines for the Classification of Films and Computer Games 2005 (the Guidelines).[192]

The following categories of Internet content are prohibited:

- Content which is, or would be, classified refused classification (RC) by the Classification Board. Such content includes:
  - child pornography;
  - excessively violent or sexually violent material;
  - sexual activity accompanied by certain offensive practices (for example, bondage);
  - bestiality; and
  - material containing detailed instruction in crime, violence or drug use.

- Content which is, or would be, classified X 18+ by the Classification Board. Such content includes real depictions of actual sexual activity between consenting adults.

- Content hosted in Australia which is, or would be, classified R 18+ by the Classification Board and is not subject to a restricted access system (preventing access by minors) which complies with criteria determined by ACMA.[193] The R 18+ classification includes:
  - material containing excessive and/or strong violence or sexual violence;
  - material containing implied or simulated sexual activity; and
  - material which deals with issues or contains depictions which require an adult perspective.

If the content is hosted in Australia and is prohibited, or is likely to be prohibited, ACMA will direct the Internet content host to remove the content from its service. If the content is not hosted in Australia and is prohibited, or is likely to be prohibited, ACMA will notify the suppliers of approved filters about the content in accordance with the Internet Industry Association (IIA) code of practice (discussed in Section 4), so that the content is blocked for users of the filter products.

If the content is 'sufficiently serious' (for example, illegal material such as child pornography), ACMA may refer the material to the appropriate law enforcement agency or to a member of the Internet Hotline Providers Association (INHOPE).[194] The international hotline may then refer the matter to the relevant law enforcement body.

[192] http://www.comlaw.gov.au/comlaw/management.nsf/lookupindexpagesbyid/IP200508205?OpenDocument.
[193] Criteria for restricted access systems are set out in the *Restricted Access Systems Declaration 1999 (No. 1),* http://www.acma.gov.au/WEB/STANDARD/pc=PC_300108.
[194] http://www.inhope.org/en/index.html.

Codes of Practice

Complementing its role in administering the complaints mechanism, ACMA is also responsible for registering and monitoring compliance with Internet industry codes of practice. The three current codes, which principally govern the activities of ISPs and ICHs, were developed by the IIA in consultation with the community and subsequently registered in May 2005.[195]

Australia was the first country to introduce Internet industry codes of practice that dealt with content matters. There are two codes for ISPs and one for ICHs. Together the codes contain a range of industry obligations to provide tools and information that assist customers in managing their access to Internet content. The codes include provisions for ISPs and ICHs to:

- assist parents and responsible adults to supervise and control children's access to Internet content;
- help ensure that internet access accounts are not provided to children without the consent of a parent or responsible adult (for example, by requiring the use of a valid credit card to open an internet access account);
- inform producers of Internet content of their legal responsibilities in relation to that content;
- inform and assist customers to make complaints about harmful Internet content;
- assist in the development and implementation of Internet content filtering technologies (including labelling technologies) and give customers information about the availability, use, and appropriate application of Internet content filtering software;
- ensure they comply with all relevant law, including reasonable requirements of law enforcement and regulatory agencies; and
- prevent access to 'usenet' newsgroups notified by ACMA as regularly containing significant amounts of child pornography.[196]

There is a graduated range of enforcement mechanisms and sanctions available to ACMA to allow flexibility in dealing with breaches of codes of practice, depending on the seriousness of the circumstances. If an ISP or ICH fails to comply with a direction by ACMA to comply with an industry code, it may be guilty of an offense.

---

[195] http://www.iia.net.au/index.php?option=com_content&task=category&sectionid=3&id=19&Itemid=33.

[196] The codes registered in May 2005 also introduced measures for certain Internet content delivered to mobile devices. Key provisions include:

- prohibition of content that is or would be classified RC or X 18+, and restricting access to content that is or would be classified R 18+ or MA 15+ to adults on an opt-in basis only;
- a requirement to inform users about the potential risks associated with the mobile environment and how to manage those risks; and
- a procedure for complaints about mobile content.

International Liaison

Due to the global nature of the Internet, international cooperation is a key requirement for effective regulation. The Act makes ACMA responsible for liaising with regulatory and other relevant bodies overseas about cooperative arrangements for the regulation of the Internet industry, including, but not limited to: collaborative arrangements to develop multilateral codes of practice and Internet labelling technologies. In the course of implementing the online content scheme, ACMA has participated in a wide variety of international regulatory forums and networks.

ACMA is a member of the Internet Hotline Providers Association (INHOPE), which is established and funded under the European Commission's Safer Internet Plus program and predecessor programs.[197] INHOPE provides a forum through which Internet hotlines are able to exchange information and experience on matters such as complaint investigation processes, occupational health and safety for hotline staff, and standardized reporting of hotline statistics. The network is also an effective mechanism for dealing with specific complaints and enhancing and complementing existing arrangements with law enforcement agencies.

Statistics

Since the implementation of the online content scheme in January 2000, ACMA has received over 5,500 complaints about Internet content, which in turn led to approximately 4,500 completed investigations. Of these, over 2,800 resulted in the identification of prohibited content, 91 percent of which contained at least one exploitative or offensive depiction of a child.

There have been over 1500 referrals to international hotlines and over 1000 to Australian police for international referral where no hotline facility is or was in operation at the time. More than 180 referrals have been made to Australian police about serious content hosted in Australia.

Regulatory Response to New Content Services

In 2005 the Australian Communications Authority and Australian Broadcasting Authority – predecessor agencies of ACMA – formalised interim safeguards for the regulation of text and audiovisual content delivered over mobile devices.[198] These interim safeguards were developed pending a review of regulatory arrangements for content on these platforms.

[197] For information about INHOPE see http://www.inhope.org/. Information about the Safer Internet Plus program is available at http://www.europa.eu/scadplus/leg/en/lvb/l24190b.htm.

[198] http://www.acma.gov.au/webwr/_assets/main/lib100039/mobile%20premium%20services%20determination%2029june05.pdf

As a result of these measures, mobile network operators and content service providers must ensure that:

- content likely to fall within the RC or X 18+ classifications is not provided on their services; and
- content likely to fall within the R 18+ or MA 15+ classifications is only available to adult customers who request it.

If customers wish to access content that is likely to fall within the classifications R 18+ or MA 15+ they must initially verify that they are 18 or older and 'opt in' to the adult service.

The *Communications Legislation Amendment (Content Services) Act 2007* (the Content Services Act) was passed by the Australian Parliament in June 2007, and commences operation in January 2008. The Content Services Act consolidates the current co-regulatory framework for non-broadcast content and expands its scope beyond stored content to include ephemeral content such as live streamed audiovisual content.

The new framework continues to build upon the regulatory principles and mechanisms provided for under the online content scheme. It imposes obligations on content service providers to ensure that content which would likely offend an average adult is not exposed to children.

ACMA will be responsible for implementing and enforcing the Content Services Act, in addition to registering and ensuring compliance with industry codes of practice which will be developed by relevant industry groups. The new codes will include procedures for parents to follow in order to supervise and control children's access to content provided across a range of new media content services, as well as to promote awareness of the safety issues associated with such services.

Criminal Laws

While ACMA deals with the potentially prohibited or prohibited material that is reported, the Australian Federal Police (AFP) and State and Territory Police Forces investigate allegations relating to the production and distribution of illegal Internet content, access to or possess of child abuse material, and use of carriage services to 'groom' children for sexual purposes.

The AFP Online Child Sex Exploitation Team (OCSET) performs an investigative and coordination role within Australia for national and international online child sex exploitation matters. OCSET examines cases presented by the Australian State and Territory Police, government and non-government organizations (including ISPs and ICHs), international law enforcement agencies, Interpol, and members of the general public.

In 2004, the Federal Government enacted the *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Act 2004*. The legislation, which came into effect on 1 March 2005, amended the *Criminal Code Act 1995* (Cth) (the Criminal Code Act) and makes it illegal to:

- use a carriage service, including by means of the Internet, to menace, harass or cause offense (maximum penalty is imprisonment for three years);
- use a carriage service, including by the Internet, to access, cause material to be transmitted, transmit, make available, publish or otherwise distribute child pornography or child abuse material (maximum penalty is imprisonment for 10 years);
- possess, control, produce, supply or obtain child pornography material or child abuse material for use through a carriage service, including by means of the Internet (maximum penalty is imprisonment for 10 years);
- use a carriage service, including by the Internet, to 'procure' or 'groom' a person who is under 16 years of age, for the purpose of engaging in sexual activity with that person or so that a third person can engage in sexual activity with that person (maximum penalties range from imprisonment for 12–15 years);

ISPs and ICHs acting solely in their capacity as an ISP or ICH are not required to monitor the actions of their customers. However, in the event that an ISP or ICH is aware that its service can be used to access particular child pornography material or child abuse material and the ISP or ICH does not refer the details of this content to the AFP within a reasonable time after becoming aware of its existence, this is considered an offense.

In addition to the criminal provisions provided for by the Criminal Code Act, all Australian States and Territories have laws governing the possession, and in some cases the dissemination, of child pornography.

3: Education and Awareness

A key component of Australia's online content scheme has been to provide information to the community, particularly to young people, about how to stay safe on the Internet. Empowering users with the appropriate knowledge, skills and tools, and providing resources for managing access to online content complements the regulatory framework.

ACMA and NetAlert Limited have worked with industry, community groups, schools, law enforcement agencies, and other government organizations to provide information and practical advice on online protection of children and families. In 2007 ACMA and NetAlert Limited merged. Additionally, in August 2007, the Australian Government announced the details of the *NetAlert - Protecting Australian Families Online (PAFO)* initiative.

The incorporation of NetAlert into ACMA brings together activities previously undertaken by the individual organizations and provides a single entity to administer these and additional programs under the *NetAlert - PAFO* initiative.

ACMA

ACMA provides advice and assistance to families on a range of Internet safety matters, through its Internet safety web site www.cybersmartkids.com.au and other related printed resources. The website provides Internet safety advice for children, parents and teachers. Features of the site include Internet safety tips, interactive quizzes, lesson plans for teachers, and links to other fun or educational sites. The site is regularly updated to encompass advice about emerging uses of networking technologies and contains comprehensive information on the use of instant messaging, webcams, blogs, and mobile phones.

In addition, ACMA has developed a series of brochures to complement the website. The brochures, each with a particular online safety message, have a similar look to the website, and again target young people and their parents or teachers. The brochures are regularly updated to accommodate changes in technology and the consumer environment, and thus far over 1.57 million copies have been distributed through school networks, community groups, the police and libraries.

Cybersmart Detectives

ACMA has worked with UK-based agencies to bring an interactive online safety activity, *Cybersmart Detectives*, to Australian schools. *Cybersmart Detectives* is an innovative online game that teaches children key Internet safety messages in a safe environment.

Children work online in real time liaising with community professionals to solve an Internet-themed problem. The activity is based in the school environment and brings together a number of agencies with an interest in promoting online safety for young people, including State and Federal Police, Internet industry representatives, and child welfare advocates.

The online medium enables teams from different schools, cities, or even countries to work together during the course of the activity. The activity encourages young people to think for themselves about what risks are associated with Internet use (particularly in chat rooms), and how they can stay safe online. Over 100 schools have participated in this activity and ACMA intends to introduce the game to many other Australian schools in order to maximize children's exposure to the online safety message. ACMA expects that by early 2008, over 30 schools across Australia will participate in the *Cybersmart Detectives* activity each week.

Cybersmart Detectives was initially developed by the UK-based child advocacy agency Childnet International, and until 2005, operated under the name of *Net*

Detectives. The activity is now independently operated by E-ngage Live. ACMA, in agreement with E-ngage Live, has adapted the activity for use in Australian schools under the name *Cybersmart Detectives*.

NetAlert Limited

In 1999, the Australian government established the not-for-profit advisory organization NetAlert Limited to provide independent advice and education about Internet safety and managing access to online content. NetAlert Limited developed and promoted information about a range of approaches for managing Internet content for users by working closely with Australian government agencies, particularly ACMA, as well as the State governments, the Internet industry, and community organizations.

Additionally, a free telephone helpline was established to provide the community with online safety information. Since August 2007 this number has also been used to assist the public in obtaining a free Internet content filter under the PAFO initiative.

Online safety resources were delivered to teachers and students at all Australian primary and secondary schools through NetAlert Limited's *CyberSafe Schools* program, and through an online safety training roadshow and information campaign named *NetAlert Expo*. The campaign was aimed at educating parents, teachers and community groups about the risks children face online. An outreach program announced under the PAFO initiative will build upon and expand this campaign.

Additionally, NetAlert Limited provided a range of online safety web resources. The NetAlert website, www.netalert.gov.au provides links to an array of online safety resources targeted to specific age groups, such as those listed below:

- www.nettysworld.com.au - Netty's World is an early learning program for children aged 2 to 7 years, which is designed to educate young children on how to use the Internet safely. It provides an interactive and safe environment for children to play in, while providing important Internet safety messages. There is a free club to join where children will receive educational resources to assist them in staying safe online.
- www.cyberquoll.com.au - CyberQuoll is an Internet safety interactive educational program for primary school children aged 8 to 12 years.
- www.cybernetrix.com.au - CyberNetrix is an Internet safety interactive educational program for secondary school children aged 13 to 16 years.
- www.wiseuptoit.com.au - Wise up to IT contains a video with four real life experiences that young people have had using the Internet. Cases include: cyber-stalking, cyber-bullying, chat room danger, and scams and identity theft.

Following the recent incorporation of NetAlert into ACMA, ACMA is considering how it can build on these and the Cybersmart resources to ensure an integrated approach to online safety.

The NetAlert - Protecting Australian Families Online (PAFO) Initiative

The *NetAlert - PAFO* initiative included $189 million to fund programs intended to provide a comprehensive response to the needs of the Australian community in protecting their families online. Several government agencies are responsible for administering these programs, including: the Department for Communications, Information Technology and the Arts (DCITA), ACMA, and the Australian Federal Police. DCITA's responsibilities include:

- an Internet safety information campaign to promote a holistic approach to protecting Australian families online through supervision, education and Internet content filters;
- a National Filter Scheme whereby every Australian household and public library will have access to a free Internet content filter to help block unwanted content; and
- a new website, www.netalert.gov.au and national telephone help line to provide advice about protecting children online, as well as access to the free filters and information about how they work.

Under the initiative ACMA will continue to provide online safety education and awareness programs and will receive additional funding to administer an expanded schools outreach program, aimed at increasing community awareness of online safety issues. ACMA's responsibilities will also include: conducting research programs to identify what young people are currently doing online; identifying how safety messages can be most effectively targeted; and regular reviewing of filtering technologies to ensure Australian families are offered the most appropriate Internet content filtering services.

Also, as part of the initiative, funding will be targeted towards developing stronger policing and enforcement measures. OCSET will be given funding for an additional 100 investigators to be added to its current staff of 35 and the Commonwealth Director of Public Prosecutions will be provided with funding to undertake the prosecutions expected to arise from the additional AFP resourcing.

4: Filter Technology and Availability

Filter technology

The online content scheme encourages the use of filtering technologies in conjunction with other online safety strategies to facilitate a safe and enjoyable online experience. It is recognized that no single measure can protect children

from online harm, and that parental supervision and guidance of children's Internet use plays an important role.

PC-Based Filters

The Internet industry codes of practice registered by ACMA as part of the online content scheme require Australian ISPs to provide an IIA 'Family Friendly Filter' to its customers. IIA Family Friendly Filters must satisfy requirements about effectiveness, ease of installation and use, configurability, and availability of support[199].

In accordance with the 'designated notification scheme' set out under the online content scheme, ACMA notifies the distributors of Family Friendly Filters about the URLs of overseas-hosted illegal and offensive content. ACMA's notifications enable distributors to update their filters to include these URLs so that an Australian end-user accessing the Internet via an accredited filter will not be able to access the illegal or offensive material. All ISPs are required to offer an accredited filter on a cost recovery basis to each new subscriber.

The recently launched PAFO initiative includes *The National Filter Scheme*. The scheme makes PC-based filters available free of charge to help tailor online protection. It includes providing a choice of Internet content filters that can be downloaded or ordered on a CD ROM for installation on a home computer.

ISP-Level Filters

Few Australian ISPs currently offer a filtered service. However, interest in ISP-level filtering technologies has increased in recent years. At the time of writing, ACMA is conducting a trial of ISP-level filtering as part of the NetAlert PAFO initiative. The trial aims to evaluate the effectiveness of the technology and its impact on ISP services, in addition to analyzing features of services currently available and ascertaining their capabilities with regard to non-HTTP based content such as peer-to-peer, instant messaging, and video streaming. The Minister of Communications, Information Technology and the Arts has instructed ACMA to report on the results of the trial by 30 June 2008.

Content filtering at the ISP level has been assessed on three previous occasions in Australia:

- A technical study was conducted by the Commonwealth Scientific and Industrial Research Organisation (CSIRO) and reported on in 2001.[200]

[199] See http://www.iia.net.au/ for further information about the selection and accreditation of IIA Family Friendly Filters.

[200] A copy of the report is available on ACMA's web site at http://www.acma.gov.au/webwr/aba/newspubs/documents/filtereffectiveness.pdf.

- A study, commissioned by the Department of Communications, Information Technology and the Arts, was undertaken by Ovum in 2003.[201]
- A technical trial was conducted by RMIT Training on behalf of NetAlert Limited in 2005.

More information about the trial of ISP-level filtering is available on the ACMA website at: http://internet.aca.gov.au/WEB/STANDARD/pc=PC_310393

Conclusion

The Australian community has enthusiastically adopted online technologies and services. The online content scheme and recent measures applying to new content services aim to address community concerns about the types of material and behaviour that children and young people may encounter online. In these co-regulatory schemes, government, industry and the community share responsibility for internet safety outcomes. Formal industry codes of practice and a statutory complaint handling mechanism are key elements of the co-regulatory framework. These co-regulatory measures are complemented by education and awareness initiatives that aim to provide online users – particularly families with children – with the tools and information to manage access to the internet for themselves and their children. Regulatory and educative measures have aimed to encourage the provision and use of filters and other access control technologies, such as restricted access systems, recognizing that technical tools can play a useful role in an effective online safety strategy.

[201] A copy of the report is available on DCITA's web site at http://www.dcita.gov.au/media_broadcasting/consultation_and_submissions/a_review_of_schedule_5_to_the_broadcasting_services_submissions_closed.

Chapter V:
Canada

by Merlyn Horton
Executive Director, Safe Online Outreach Society (SOLOS)
Mission, British Columbia, Canada
and
Jay Thomson
Assistant Vice President, Broadband Policy, TELUS Communications Company
Ottawa, Ontario, Canada

Overview

Rather than addressing concerns about online safety issues and access to objectionable online material through legislation, Canada has chosen to emphasize and promote self-regulation. This approach focuses particularly on public and private sector initiatives that build public awareness, and educate consumers and empower Internet users with technological tools such as filters to protect themselves and their families in a manner they deem most appropriate in their own particular circumstances.

Although published almost seven years ago, the most comprehensive expression of the Canadian approach in this regard remains a 2001 booklet issued by the federal Department of Industry (Industry Canada) entitled "Illegal and Offensive Content on the Internet: The Canadian Strategy to Promote Safe, Wise and Responsible Internet Use" (also known as the "CyberWise Strategy").[202]

It states in that document:

> "Although Canada has strong laws that apply to cyberspace, the Government of Canada recognizes that legislation alone will not solve the problems of illegal and offensive content on the Internet. Legislative reform is important, but the federal government's approach is to involve a broad spectrum of Canadians in addressing the issues. Its priorities include:
>
> - supporting initiatives that educate and empower users;
> - promoting effective industry self-regulation;
> - strengthening the enforcement of [existing] laws in cyberspace;
> - implementing hotlines and complaint reporting systems; and
> - fostering consultation between the public and private sectors, and their counterparts in other countries." [203]

The 23-page document concludes:

[202] Government of Canada, "Illegal and Offensive Content on the Internet: The Canadian Strategy to Promote Safe, Wise and Responsible Internet Use," http://cyberwise.ca/epic/site/cybpr-cybi.nsf/en/h_wd00089e.html, p. 5.
[203] Ibid, p. 5.

> "Overall, Canadian parents believe that the job of managing Internet content is a responsibility they share with Internet service providers, Internet users, independent organizations, governments, website producers and police. Schools and libraries, too, play a key role, and Canadians will continue to reach far beyond international borders to develop effective solutions, share experiences and make a difference here at home. By working collaboratively, Canadians are creating a healthy environment in which to teach Canada's children to be the safe, wise and responsible Internet users of the future."[204]

This chapter attempts to provide a comprehensive, although not exhaustive, summary of the variety of Canadian public and private Internet safety initiatives, currently in effect, which contribute to creating the healthy environment Canada continues to seek for its young netizens.

Basic Stats

Canada is one of the most heavily wired nations in the world, with approximately 70 percent of Canadian households (8.7 million) online. 60 percent of Canadian households (7.5 million) subscribe to a high speed service, in most cases from one of the four major telephone companies or cable companies, which collectively hold 67 percent of the market.[205]

According to a 2006 report[206] by the Canadian youth marketing consultancy, Youthography,[207] which was submitted by a group of Canadian telecommunication companies[208] as part of a Canadian Radio-Television and Telecommunications Commission (CRTC) proceeding[209], 97.9% of Canadian 9 to 13 year olds have Internet access in their home, with 81.8% of them having high speed. For youth aged 14 to 18, the corresponding numbers are 99.3% and 83.8% respectively. The report found that the younger age group spent an average of 10.3 hours/week online, whereas the older group was online an average of 18.6 hours/week.

---

[204] Ibid, p. 19.

[205] CRTC, "CRTC Telecommunications Monitoring Report, Status of Competition in Canadian Telecommunications Markets and Deployment/Accessibility of Advanced Telecommunications Infrastructure and Services," July 2007, http://www.crtc.gc.ca/eng/publications/reports/PolicyMonitoring/2007/tmr2007.pdf, p. 60-73. The four major companies are the telcos, Bell Canada and TELUS, and the cable companies, Rogers and Shaw.

[206] The report can be found at: http://support.crtc.gc.ca/applicant/docs.aspx?pn_ph_no=pb2006-72&call_id=41190&lang=E&defaultName=Bell,%20MTS%20Allstream,%20SaskTel%20and%20Telus&replyonly=&addtInfo=&addtCmmt=&fnlSub=.

[207] www.youthography.ca

[208] The companies involved were: Bell Canada, MTS Allstream, SaskTel and TELUS.

[209] The CRTC proceeding is available at: http://www.crtc.gc.ca/archive/ENG/Notices/2006/pb2006-72.htm. Information on the CRTC can be found at: www.crtc.gc.ca.

Published before the popularity of social networking and user-generated content sites really took off in Canada, the Youthography 2006 report found that the most common online activities for all youth ages 9 to 24 were email, web surfing and researching information for school or work. The 14 to 24 age group also responded that they used the Internet for instant messaging. The report also indicated that the youngest age group (9 -13) were far less likely to be emailing and more likely to be playing videogames.

A similar survey conducted today would no doubt find that Canadian youth are spending much more of their online time with social networking sites like Facebook and user-created content sites like YouTube. Indeed, Facebook is very popular in Canada and Canadians as a whole represent a surprisingly large portion of Facebook's user base.[210]

More recent surveys indicate that Canadian parents are struggling to find resources to help keep their kids safe online. For example, a news release[211] summarizing the results of a survey commissioned last summer by Symantec Corp. indicated that just over half of Canadian parents (58 percent) know where to download parental control software and only one third (36 percent) are actually using parental controls for their children's Internet browsing. The release also notes that the survey found that of the possible online threats children can encounter, 77 percent of Canadian parents are concerned about sexual predators, 74 percent are worried their kids will come across pornographic sites, and 70 percent fear their children will fall victims to fraudulent scams.

Similarly, a survey[212] of Quebec parents, commissioned around the same time by Quebec-based communications company Videotron Ltd.[213], highlighted the differences between what parents think their kids are doing online and what their kids are actually doing. For example, the Videotron survey found that, while only 8% of parents think their teens have used a webcam to chat with strangers, 27% of teens admitted to actually having done so. Also, while 80% of Quebec parents indicated they dictate rules for Internet use, only 52% said they regularly discuss such rules in the home.[214]

Legislation

With only a few exceptions, Canada does not have any "Internet" laws. The Canadian approach is generally "if it is illegal offline, it is illegal online;" therefore no direct or even indirect legislative references to the Internet are deemed necessary. However, there are certain provisions of the "Canadian Criminal

[210] http://blog.facebook.com/blog.php?post=2398302130. See also http://www.thoughtballoons.net/?p=156.
[211] http://www.newswire.ca/en/releases/archive/July2007/25/c9172.html
[212] http://www.vigilancesurlenet.com/en/initiatives/2007-survey.php
[213] http://www.videotron.com/services/Home.do?to=index
[214] http://www.canada.com/montrealgazette/news/business/story.html?id=7a2595b0-590e-4af0-9d09-3763f102116d&k=92741

Code" which make transmitting and accessing of child pornography a criminal offence.[215] Additionally, there are other Criminal Code provisions which establish judicial take-down regimes for child pornography[216] and hate propaganda[217] that are "stored on and made available through a computer system." Also, the "Canadian Human Rights Act" makes communicating hate messages "by means of a computer or a group of interconnected or related computers, including the Internet…" an offence.[218]

Education and Awareness Efforts[219]

Federal Government Education and Awareness Efforts

Canada's "National Strategy to Protect Children from Sexual Exploitation on the Internet" (the National Strategy), announced in 2004, was developed and is delivered through Public Safety Canada (PSC) and provides $43 million over five years to ensure a comprehensive, coordinated approach to protecting children on the Internet and for pursuing those who use technology to prey on them.[220]

The National Strategy is delivered in partnership with three federal organizations: PSC; Industry Canada (through its SchoolNet program); and the Royal Canadian Mounted Police (RCMP). It has three main objectives: enhancing enforcement capacity; providing public reporting and education to prevent victimization and; developing partnerships with the e-learning industry, the private sector and other levels of government to foster effective public awareness, education and crime prevention strategies.[221]

Fundamental to the government's approach are: initiatives that educate and empower users; effective industry self-regulation; and industry-law enforcement cooperation. Integral to its efforts are: dialogue and consultations with the public and private sectors; international collaboration with other governments; and research and analysis to better understand the scope of the issues and the range of available solutions.

CyberWise.ca

As part of the National Strategy, federal funding was provided to Industry Canada to launch CyberWise.ca,[222] which is now the centralized, comprehensive source

[215] http://www.canlii.org/ca/sta/c-46/sec163.1.html
[216] http://www.canlii.org/ca/sta/c-46/sec164.1.html
[217] http://www.canlii.org/ca/sta/c-46/sec320.1.html
[218] See: http://www.chrc-ccdp.ca/discrimination/watch_on_hate-en.asp. As far as the authors know, this is the only piece of Canadian federal legislation which uses the word "Internet".
[219] Descriptions of the various initiatives are taken in large part from the corresponding websites themselves.
[220] http://www.sp-ps.gc.ca/media/bk/2005/bg20050124-eng.aspx
[221] http://www.psepc.gc.ca/prg/le/oce-en.asp
[222] www.cyberwise.ca

for the federal government's educational resources on Internet safety.[223] The site provides tips, resources and useful links for parents, teachers, youth professionals, kids (4 to 10), and teens (11 to 17) on how to use the Internet safely. Among other things, the site offers a chat dictionary, classroom activities, kids' games, and descriptions of online dangers such as cyberbullying, child pornography and luring.

The CyberWise initiative seeks to promote the safe use of the Internet through the creation of learning activities and other online resources, and through distribution of its brochure, its two posters, two bookmarks and a one-page leaflet. Since January 2006, CyberWise.ca has distributed, on request, several thousands of their materials to schools and Canadians in general.

Internet 101

In the fall of 2004, members of the RCMP and local and provincial police forces based in the National Capital Region teamed up to offer a multi-media presentation for youth and their parents regarding the potential dangers of the Internet, and how they can be safely avoided. The event, which also promoted the simultaneous launching of the Internet 101 website in French, was attended by over 400 youth and their parents.[224]

Based on the success of the first event and continued demand from the public for education on Internet safety, a new organizing committee was established in Ottawa to put on a second workshop. The RCMP joined with the Department of National Defence's Military Police and local and provincial police based in Ottawa to present Internet 101 at a movie complex in the spring of 2005. At the same time, the English version of the website[225] was launched in order to continue providing assistance to parents and educators to ensure that youth surf safely.

Internet 101 is not intended to replace other online resources, but is rather to be a gateway to existing websites, which are recognized and used by police themselves. It is also a collection of presentations, safety tips and other resources contributed by educational partners for the benefit of parents, teachers and police across Canada.

The resources on the Internet 101 website are divided into three categories, with information and activities targeted to the following demographics: tools for youth (8 to 10), (11 to 13) and (14 to 17), tools for parents and tools for educators.

[223] Responsibility for the cyberwise.ca website is to be transferred at some point from Industry Canada to Public Safety Canada.
[224] http://www.internet101.ca/fr/index.php
[225] http://www.internet101.ca/en/index.php

In February 2007, Industry Canada and the RCMP went on a cross Canada tour to promote "Kit101: An Educator's Guide to Internet Safety".[226] This kit was created to provide educators, youth professionals, parents and students with tools and tips for avoiding dangers on the Internet. Kit101 contains dynamic interactive presentations on true stories, a brochure full of information on where to find additional resources to accompany the workshops, educational materials, and flash cards on Internet safety. In short, it is a workshop in a box.

Provincial Government Education and Awareness Efforts

In 2006, the government of Alberta Department of Children's Services committed $6.2 million to address child sexual exploitation, $400,000 of which is dedicated to public awareness activities.[227] In May 2006, Alberta Children's Services launched www.wereon2u.ca, a hard-hitting Internet safety website for teens. Shortly thereafter, the department launched a site for younger children called www.badguypatrol.ca.

The Alberta government has also developed a number of new resources to address bullying, in its many forms, including cyberbullying. Younger children can learn how to handle bullying by visiting www.teamheroes.ca while older children can learn how to stand up to and stop bullying by visiting www.b-free.ca. Additionally, parents can find information and practical advice at www.bullyfreealberta.ca. Alberta also provides a toll-free phone number for anyone needing immediate advice and support.

As part of its larger “Provincial Strategy to Protect Children from Internet Crimes”, launched in 2004, the government of Ontario announced in January 2005[228] that it would provide Grade 7 and 8 classrooms in the province with new interactive software, called “CyberCops”,[229] to help students learn to be safe online and protect themselves from Internet stalkers. One CyberCops program, entitled “Mirror Image”,[230] was distributed in both English and French to approximately 3200 Ontario schools in January 2006 and roll-out to schools of a second program, called “Air Dogs”[231], began in February 2007. The first program teaches students to recognize techniques used by criminals on the Internet; the second focuses on themes of cyber-theft, extortion and bullying. The Ontario Physical

[226] http://strategis.ic.gc.ca/epic/site/cybpr-cybi.nsf/en/wd00135e.html
[227] http://www.gov.ab.ca/acn/200606/20025A573C720-D1B8-8CF6-A88342AFA9F92212.html
[228] www.attorneygeneral.jus.gov.on.ca/english/news/2005/20050121-protkids.asp
[229] CyberCops (http://www.cybercops.net/cybercops/) was created by LiveWires Design Ltd. of Vancouver (www.livewwwires.com), with content developed in partnership with the Ontario Provincial Police.
[230] http://www.cybercops.net/cybercops/games/mirrorimage/
[231] Information on the “Air dogs” program and its distribution to Ontario schools can be found in press releases at: http://www.ophea.net/ophea/Ophea.net/CyberCops.cfm and http://ogov.newswire.ca/ontario/GPOE/2007/04/30/c2562.html?lmatch=&lang=_e.html.

and Health Education Association (OPHEA)[232] developed a teacher resource package and training materials[233] to assist teachers to integrate the material into the classroom.

Non-Governmental Organizations

This section highlights the most visible and well-known Internet safety education and public awareness initiatives launched and operated by Canadian non-governmental organizations. There are many others on a smaller scale,[234] which undoubtedly make a valuable contribution;[235] however it is beyond the scope of this report to cover all of them.

The Media Awareness Network[236]

Supported by a number of leading Canadian communications companies[237], the Ottawa-based "Media Awareness Network" (MNet) is an internationally-recognized and award-winning Canadian not-for-profit centre of expertise and excellence in media education. Its objective is to ensure children and youth possess the necessary critical thinking skills and tools to understand and actively engage with media. MNet's comprehensive website offers extensive resources and support materials "for everyone interested in media and information literacy for young people."[238] This includes Internet literacy.

MNet began studying the implications of the Internet for young people in 1996, and in 1999 launched Web Awareness Canada.[239] This program uses a unique delivery model based on partnerships with public libraries, the education sector, parent groups, and community organizations. Its primary focus has been to ensure teachers and librarians are up to speed on the issues emerging as young people go online. It does this by licensing workshop tools covering topics such as: online safety, cyberbullying, protecting personal privacy, authenticating information, marketing to young people,[240] and online hate.[241]

---

[232] The association is a provincial non-profit organization "committed to working collaboratively with various organizations to advocate for and support active healthy school communities in Ontario." See: http://www.ophea.net/.
[233] For the CyberCops teacher resources, see: http://www.ophea.net/Ophea/Ophea.net/CyberCopsResources.cfm.
[234] A Google search of Canadian sites with regard to "Internet safety" yields over 2 million results. Many, if not the vast majority, of the sites listed (they have not all been reviewed) make reference or link to the sites highlighted in this report.
[235] For example, see: www.cyberbullying.ca.
[236] www.media-awareness.ca
[237] Supporters include Bell Canada, CTVglobemedia, Microsoft Canada, TELUS, and Rogers Yahoo! MNet also receives funding from the government of Canada.
[238] http://www.media-awareness.ca/english/index.cfm
[239] http://www.media-awareness.ca/english/special_initiatives/web_awareness/index.cfm
[240] http://www.media-awareness.ca/english/catalogue/products/descriptions/wa_tea.cfm

MNet resources for parents[242] include a comprehensive companion Internet safety website www.bewebaware.ca and a workshop available for presentation in schools and community centres called "Parenting the Net Generation".[243]

To support its Internet safety programs, MNet conducts original research on Canadian children's Internet use. The "Young Canadians in a Wired World" research project,[244] launched in 2000, is the most comprehensive and wide-ranging study in Canada investigating the behaviors, attitudes, and opinions of students with respect to the Internet.

Canadian Centre for Child Protection[245]

Also supported by leading Canadian communications companies,[246] the recently-launched "Canadian Centre for Child Protection", based in Winnipeg, brings under one physical and virtual roof various provincial and national child safety initiatives previously operated under the banner of Child Find Manitoba. These include:

- **Cybertip.ca**[247] - Canada's tipline for reporting the online sexual exploitation of children;[248]
- **Kids in the Know**[249] - an interactive safety education program for increasing the personal safety of children (kindergarten to high school) and reducing their risk of sexual exploitation;[250]
- **Stop Sex With Kids**[251] - an initiative which through education, advocacy, and reporting provides the public with information on how to take action against child exploitation through prostitution; and
- **Child Find Manitoba**[252] - a program that assists in the location of missing children in the province of Manitoba and works with the Child Find network throughout Canada.

---

[241] See: http://www.media-awareness.ca/english/catalogue/products/descriptions/online_hate.cfm. Information can also be found at: http://www.media-awareness.ca/english/issues/online_hate/index.cfm.
[242] http://www.media-awareness.ca/english/parents/index.cfm
[243] http://www.media-awareness.ca/english/catalogue/products/descriptions/parenting_net_generation.cfm
[244] http://www.media-awareness.ca/english/research/YCWW/index.cfm
[245] www.protectchildren.ca
[246] The Founding Partners of the Centre are Bell Canada, Honeywell, Shaw Communications and TELUS. The Centre also receives funding from the government of Canada.
[247] www.cybertip.ca
[248] Funding for Cybertip.ca is provided by the Canadian government, Bell Canada, Microsoft Canada, Rogers Communications, Shaw Communications, TELUS, MTS Allstream, AOL Canada, Computer Associates, and Cogeco.
[249] http://www.kidsintheknow.ca/app/en/
[250] Kids in the Know receives funding from the government of Canada (through SchoolNet), Honeywell and Microsoft Canada.
[251] www.stopsexwithkids.ca
[252] www.childfind.mb.ca

The Canadian Centre for Child Protection website provides access to Internet safety information through links to its signature programs, Cybertip.ca and Kids in the Know. The Cybertip.ca website identifies risks for children on the Internet; addresses online safety and child development, children's online interests and chat lingo; and offers Internet safety guidelines and advice on how parents can get involved in their children's online activities.[253]

The Kids in the Know site offers a protective factors checklist for online safety,[254] as well as a downloadable comic book for classroom use called "Zoe and Mollie Online".[255] Accompanied with teacher resources, the comic, created for Grade 4 students, addresses risks associated with children sharing personal information and sending pictures online.[256]

Safe Online Outreach Society (SOLOS)[257]

The purpose of the British Columbia-based SOLOS[258] is to educate the public about exploitation on the Internet. This is accomplished by conducting research, creating materials and delivering presentations and workshops that will train youth, professionals and parents on how to recognize and respond to online sexual exploitation and assist children and youth affected by this issue.

SOLOS has produced a 100-page curriculum, an Organizational Assessment Tool, three eight-page youth Internet safety booklets, an interactive CD for youth, a Youth-2-Youth peer mentoring program, and has developed presentation materials for adults, professionals and youth. During 2006, SOLOS held over fifty presentations reaching 3500 participants in British Columbia and its materials were distributed to over 130 agencies, including: school districts, community policing offices, research centers, and community based crime prevention organizations.

Kids Internet Safety Alliance[259]

Focused primarily on the online sexual exploitation of children and youth, the Kids' Internet Safety Alliance (KINSA)[260] was inaugurated in 2005, combining expertise in law enforcement, prosecution, business and technology to provide "an aggressive and proactive response to the negative aspects of the Internet that harm young people."

[253] http://www.cybertip.ca/en/cybertip/inet_safety_tips
[254] http://www.kidsintheknow.ca/app/en/direct_protective
[255] http://www.kidsintheknow.ca/PDFS/zoemolly_comic.pdf
[256] Grade 4 was chosen as the target audience based on data indicating that by Grades 5 and 6 children are building online relationships and sending pictures.
[257] www.safeonlineoutreach.com
[258] SOLOS has received funding from the government of British Columbia and TELUS.
[259] www.kinsa.net
[260] KINSA has received funding from the government of Ontario.

In the summer of 2007, KINSA and the Canadian youth specialty TV channel YTV[261] partnered to provide a fun and informative way for kids to learn about smart surfing. KINSA's "Surf Smart"[262] was built into "Sitekick",[263] a popular YTV online community-based game, to give kids the opportunity to collect limited edition KINSA-branded Surf Smart chips while learning about online safety. To get the chips, children have to read Internet safety tips.[264] As players earn more chips, they increase their ranking in the online community.

Industry Education and Awareness Efforts

Consistent with the emphasis in Canada on self-regulation, Canada's major Internet companies not only support the NGOs listed above, but also directly offer their customers Internet safety information and/or inexpensive or free tools (parental controls) through their corporate and consumer websites.

- **Bell Canada** offers an extensive Internet safety site, in both English and French at: http://safety.sympatico.msn.ca/
  - Additionally, parental controls are accessible at: http://service.sympatico.ca/index.cfm?method=content.view&category_id=583&content_id=7300.
- **Cogeco** provides parental controls at: http://www.cogeco.ca/en/faq_children_security_o.html
- **MTS Allstream** has parental controls accessible at: http://www.mts.ca/portal/site/mts/menuitem.a275cbc6dbb0d4e50e1408103124 8a0c/?vgnextoid=af3c854590323010VgnVCM1000000408120aRCRD&vgnext channel=152ecc878fc81010VgnVCM1000000408120aRCRD
- **Rogers Communications** makes parental controls available at: http://www.shoprogers.com/store/cable/internetcontent/features/security_pare ntalcontrols.asp?shopperID=X87MH9UGNN368JVVD4JTFP2709PMC4PE.
- **Shaw Communications** offers safety tips at: http://start.shaw.ca/Start/enCA/Customer+Service+Centre/Internet+Safety/10T hingsToProtectYour+Kids.htm
  - Safety FAQs can also be found at: http://start.shaw.ca/Start/enCA/Customer+Service+Centre/Internet+Safety/Kid sFAQs.htm

  Parental controls can be found at: http://www.shaw.ca/en-ca/ProductsServices/Internet/No+Cost+Extras/ SecureExtended.htm.
- **TELUS** has parental controls available at: http://www.mytelus.com/internet/security/TELUSsecuritycontrol.do

[261] www.ytv.com
[262] http://www.ytv.com/etc/kinsa
[263] http://www.ytv.com/sitekick/index.asp?lid=
[264] http://www.ytv.com/etc/kinsa/

- Launched in June 2006, **Videotron**'s extensive Internet safety site, available in French and English, which includes information on its "Vigilance on the Net" campaign, can be found at www.vigilancesurlenet.com.[265]

Other Technology Solution Providers

The authors have reviewed the comprehensive description of operating system filters and web browser controls, as well as PC-based filters and monitoring tools, which is included in Adam Thierer's chapter on the state of online safety initiatives in the United States.[266] Although each of the numerous Internet filtering and monitoring software tools which Professor Thierer has listed have not been investigated by the authors of this chapter, it is presumed that the filters, controls, and tools are all as equally accessible and available to Canadian Internet users as they are to Americans. Thus, there is no need to repeat them here.

The Cybertip.ca website also provides Canadians with an extensive list of filtering software tools available to them,[267] including some tools not listed by Professor Thierer. The compilation and online publication of this list was one of the first initiatives of the multi-stakeholder "Canadian Coalition Against Internet Child Exploitation" (CCAICE), which was formed in 2004 to establish and implement a multi-faceted national action plan to help in the fight against the sexual abuse and exploitation of children on the Internet.[268]

The authors note that Netsweeper,[269] which is included in Professor Thierer's list, is a Canadian company based in Guelph, Ontario. Radialpoint[270] is another Canadian company offering filtering software.[271] A number of Canadian ISPs use either Netsweeper's or Radialpoint's software for their re-branded parental controls.

Conclusion

The data referenced above shows that there is an obvious (and, unfortunately, unsurprising) discrepancy between what Canadian parents think their kids are doing online and what their kids actually do. It also appears that there is a divergence between the apparent inability of these parents to find the Internet

[265] A press release about Videotron's "Vigilance on the Net" campaign can be accessed at: http://www.vigilancesurlenet.com/en/pdf/pr_vigilance.pdf.
[266] See Chapter 1, p XX - XY.
[267] http://www.cybertip.ca/en/cybertip/information_for_parents/
[268] See http://www.cybertip.ca/PDFs/en/media_releases/CCAICE_pressrelease_e.pdf and http://www.cybertip.ca/PDFs/en/media_releases/CCAICE_backgrounder_e.pdf.
CCAICE membership includes Canada's major ISPs and the Canadian Association of Internet Providers (CAIP), Cybertip.ca, the RCMP and other law enforcement agencies, and representatives from the federal and provincial governments.
[269] www.netsweeper.com
[270] http://www.radialpoint.com/en/home/home.php. Radialpoint is based in Montreal, Quebec.
[271] www.freedom.net

safety information they want and the amount of such information actually made available online by Canadian public and private sector stakeholders. While the number of Canadian online safety information sites might not equal that of the US, the Canadian sites that do exist, as summarized above, are incredibly comprehensive and offer parents, educators and kids easily accessible one-stop shops for the online safety information required. The reason why Canadian parents are apparently not finding online safety information therefore is not a result of lack of quantity or quality options.

Perhaps the difficulty arises because the information itself is online and those parents who are unable to find it are themselves still uncomfortable using the Internet. Canadian parents who are comfortable with the Internet should easily find safety information, either by simply going through their ISP's website in many cases or by conducting a simple online search for Canadian resources in this area. Accordingly, it is surmised that "offline" parents have the most difficulty finding online Internet safety resources. Assuming this is the case, the challenge would be to find ways to use offline tools to educate offline parents about their kids' online activities. Otherwise, perhaps the onus should be on parents to develop their online skills and knowledge to a level sufficient enough to use and understand the valuable online safety resources that are widely available to them.

Despite the challenge of ensuring Canadian parents and educators have access to, *and use*, the comprehensive online safety information available to them, the authors continue to support the Canadian strategy which promotes education, public awareness and industry self-regulation in place of legislation. As numerous others have stated on many occasions, the government cannot legislate good parenting, and we agree. If there is any place for legislating in this area, we would strongly suggest that all Canadian provinces and territories establish Internet safety education as a mandatory component of school curricula (a matter of provincial/territorial jurisdiction), and provide their teachers with both the resources and the time to develop and present lessons in this regard. In today's online world, online safety education should receive equal status as other school subjects, to help ensure our young people are safe, wise and responsible Internet users.

Chapter VI:
Austria

by Michael Eisenriegler
and
Romana Cravos
Internet Service Providers Austria, Austria

Overview

In many instances, the child protection legislation in Austria is very similar to that of Germany. Austrian attorneys even cite German rulings in Austrian courts. However, this is not at all the case with online safety and child protection. While Germany continues to enforce its very strict laws and policies, there are still no Internet-specific regulations on this matter in Austria. Child protection in Austria, and to some degree in Germany, is mainly subject to provincial legislation. The current Austrian government plans to take the responsibility for child protection away from the provinces and introduce federal laws, but probably not before 2009. It is also unknown as of now, if these laws will include any specific regulations concerning the Internet.

Basic Statistics

Total population: 8,298,923[272]

- 0 – 19 years: 1.791.042
- 5 – 9 years: 416,818
- 10 – 14 years: 478,400
- 15 – 19 years: 496,324

General

69.4% of the Austria population between 16 and 74 years has used the Internet in the last 12 months.[273] 70.7% of Austrian households own a computer and

[272] Statistik Austria
(http://www.statistik.at/web_de/statistiken/bevoelkerung/bevoelkerungsstand_jahres-_und_quartalswerte/bevoelkerungsstruktur/023458.html
(23.5.2007)
and
http://www.statistik.at/web_de/static/bevoelkerung_zu_jahresbeginn_seit_2002_nach_fuenfjaehrigen_altersgruppen_u_023468.pdf (23.5.2007)

[273] Statistik Austria, "Internetnutzer und Internetnutzerinnen 2007," June 18, 2007, http://www.statistik.at/web_de/static/internetnutzer_und_internetnutzerinnen_2007_022211.pdf

59.6% of Austrian households have internet access.[274] 90.3% of Austrian households have mobile phones.[275]

Minors

Internet Access

- 6 years: 21%[276]
- 7 years: 34%
- 8 years: 34%
- 9 years: 53%
- 10 years: 78%

Using a Mobile Phone

- 6 years: 6%[277]
- 7 years: 7%
- 8 years: 23%
- 9 years: 34%
- 10 years: 65%

Time of Day of Computer Usage

- Afternoon: 63%[278]
- Evening: 12%
- After school: 7%
- Weekend only: 6%
- Before school: 1%

Where They Use the Internet

84% of the children use the Internet at home.[279]

[274] Statistik Austria, "Haushalte mit Computer und Internetzugang 2002-2007," September 27, 2007, http://www.statistik.at/web_de/static/haushalte_mit_computer_und_internetzugang_2002-2007_022206.pdf
[275] Statistik Austria, "Haushalte mit Festnetzanschluss und Mobiletelefon 2007," June 18, 2007, http://www.statistik.at/web_de/static/haushalte_mit_festnetzanschluss_und_mobiltelefon_2007_022209.pdf
[276] Bildungs Medien Zentrum des Landes Oberösterreich, " 1. Oö BIMEZ Kinder-Medien-Studie 2007," (23.3.2007), http://www.bimez.at/uploads/media/pdf/medienpaedagogik/kinder_medien_studie07/charts_kinder.pdf
[277] 1. Oö BIMEZ Kinder-Medien-Studie 2007.
[278] 1. Oö BIMEZ Kinder-Medien-Studie 2007.
[279] 1. Oö BIMEZ Kinder-Medien-Studie 2007.

When Children Use the Internet

53% of children use the Internet in the afternoon. 18% use it in the evening. Children who use the Internet on weekends only equal 10%. 8% use it at lunchtime or after school.[280]

Duration of Internet Use

32% of minors use the Internet up to 30 minutes a day. 11% use it between 30 and 60 minutes a day. Only 5% use the Internet for more than 60 minutes a day. 41% of minors who responded stated they rarely used the Internet.[281]

Who Children Use the Internet With

24% of children said they used the Internet with their mothers. 21% use the Internet with their friends. Children using the Internet with their fathers equal 20%. 13% use it with their brothers and sisters.[282]

Why They Use the Internet

The main reasons children gave for using the Internet were: watching special sites for kids; searching for certain information; searching for information for school; playing online games by themselves; writing emails; watching films and videos; and chatting.[283]

Where They Obtain Information on Internet Sites

They get their information from: television, friends, their parents, and their brothers and sisters.[284]

Education and Awareness Efforts

Austria is a good example of well functioning Internet industry self-regulation, where the industry cooperates closely with state authorities and all other stakeholders, such as NGOs, social scientists, school officials, and parents' organizations. The Austrian Internet industry is represented by ISPA (Internet Service Providers Austria).

[280] 1. Oö BIMEZ Kinder-Medien-Studie 2007.
[281] 1. Oö BIMEZ Kinder-Medien-Studie 2007.
[282] 1. Oö BIMEZ Kinder-Medien-Studie 2007.
[283] 1. Oö BIMEZ Kinder-Medien-Studie 2007.
[284] 1. Oö BIMEZ Kinder-Medien-Studie 2007.

Austrian Child Protection Initiatives

Stopline

As early as 1998 ISPA started to establish a private telephone- and Internet-hotline to deal with child pornography and neo-Nazism on the Internet. Stopline (http://www.stopline.at) works in tandem with similar services all over the world, as well as with the government hotline run by the Austrian Home Ministry. It is partly funded by European funds and operates within the framework of the EU's INHOPE program.

Saferinternet.at

ISPA is project partner of the Austrian Institute for Applied Telecommunications (ÖIAT) and together they run Austria's Safer Internet node (Saferinternet.at). Saferinternet.at publishes a very informative website aimed mainly at parents and teachers, produces educational material, and through their advisory board maintains close relationships with all stakeholders, especially from industry and government. Saferinternet.at is funded by the EU, by various institutions of the Austrian government, and by some key players of the Austrian Internet industry.

Brochure "Safer Surfing"

The 60-page brochure "Safer Surfing" was originally produced by ISPA for teenagers to explain various risks of Internet usage. It turned out that it was not only popular with its target audience but also with their parents and teachers. Since the original printing, several variations and updates have come out or are currently in production, one of which is in cooperation with Saferinternet.at. Current ideas for the future development of this brochure include the setup of a Wiki and a supplement with legal FAQs for answering problems specific to the use of the Internet in schools.

FOSI PoP

In 2007, ISPA became an official Point of Presence of FOSI in Austria. ISPA aims to promote the ICRA labeling system among Austrian content providers and, in a later stage, among end users through parents' organizations, religious institutions and other NGOs. They will have the possibility to publish ICRA filter presets according to their respective value system. These presets can then be used by parents with an ICRA filter plugin, which is planned to be developed for Internet Explorer and Firefox browsers. ISPA aims to establish the ICRA filter as the foremost child protection system in Austria within the next two years.

Sicher-im-Internet.AT

Another private initiative for promoting the safe use of the Internet in Austria is Sicher-im-Internet.AT (Security in Internet). It was originally started by Microsoft and is now being supported by several companies, NGOs and ministries. The main focus of this initiative lies on promoting technical security for IT and the Internet in order to tackle issues like viruses and phishing, but it will also offer specific recommendations for parents.

PEGI Online

The Pan European Game Information (PEGI) System makes it possible for parents to know which computer games are suitable for their children. With a specific age classification that uses special symbols, the PEGI System offers a detailed description of content. In addition to the PEGI System, PEGI Online was created in order to protect children from unsuitable online game content. If an online game meets the requirements of the PEGI Online Safety Code, the game provider is allowed to use the PEGI Online Logo. PEGI is funded within the scope of the European "Safer Internet" Program.

Child- and Teen-Oriented Websites in Austria

Alles über Nachhilfe (www.nachhilfe.at)
Computerschule für Kinder (www.profikids.at)
Der Clown Habakuk (www.clown-habakuk.at)
English for kids (www.e4kids.co.at)
Family Entertainer (www.robertsteiner.at)
Figurentheater Lilarum (www.lilarum.at)
Gendarm für Kinder (www.inspektorlux.at)
Info-Seiten für Kids (www.kidsweb.at)
Jolly Schreibwaren (www.jolly.at)
Kidz World (www.kidzworld.at)
Kinderbuchautorin Mira Lobe (www.miralobe.at)
Kinder-Evangelisations-Bewegung (www.entdecker-kids.at)
Kinderkurier (www.kiku.at)
Kinderland (www.kinderlandwien.at)
Kinderschutz (www.kinderpolizei.at)
Kindersicherheitsclub (www.helmi.at)

Kinder Business Week (www.kinderbusinessweek.at)
Kinder Filmfestival (www.kinderfilmfestival.at)
Kirango – Büchereien (www.kirango.at)
Lieblingsbücher von Kindern (www.lesemaus.at)
Mamilade (www.mamilade.net)
Musikvideowettbewerb (www.videostars.at)
Österreichische Beamtenversicherung (www.oebv4kids.at)
Österreichischer Buchklub der Jugend (www.buchklub.at)
Portal für Kinder (www.kinder.at)
Rechte für Kinder (www.kinderrechte.gv.at)
Reise- und Ausflugsziele in Österreich (www.reisenmitkindern.at)
Sagensammlung online (www.sagen.at)
Seite für Tierliebhaber (www.zoo4kids.at, www.stars4kids.at)
Stadtprogramm für Kids (www.wienxtra.at)
Tate - Society to support bright children (www.tate.at)
Theater und Kultur (www.ichduwir.at)
Unicef (www.unicef.or.at)
Universität für Kinder (www.kinderuni.at)
Vier pfoten Kinder- und Jugend-Site (www.pfoetchen.at)
Webauftritt der Kinderzeitschrift Weite Welt (www.weitewelt.at)
Wettbewerb zur Sicherheit (www.sicherheit-fuer-alle.at)
Wiener Volkshochschulen (www.vwv.at)
WWF Österreich (www.pandazone.at)
Zoo Vienna (www.zoovienna.at)
Zoom Kindermuseum (www.kindermuseum.at)

Conclusion

ISPA Austria believes that the approach of FOSI to online safety is non-partisan and democratic, as well as effective, because it involves parents on one side and content providers on the other. The protection of children should never be an excuse for censorship, either directly by the government or through access providers. On the other hand, the Austrian Internet industry acknowledges that there is still a lot of education and empowerment to be done, because a functioning democracy needs informed citizens. That is why ISPA commits itself to the continued education of parents, teachers, kids and government officials to ensure that freedom of expression and the need for protection of minors are not two principles conflicting with each other.

Chapter VII:
The Netherlands

by Marjolijn Bonthuis, Senior Advisor
and
Marjolijn Durinck, Advisor
ECP.NL[285]/Digibewust (Digitally Aware)
The Netherlands

Overview

Demographic Information

The Netherlands has over 16 million inhabitants. As of January 1, 2006 the number of youngsters (25 and younger) equalled almost 5 million and there were approximately 2.4 million seniors (65 years or older).[286]

Internet Usage and New Technologies

In the Netherlands, Internet has become a widely spread and accepted technology. A vast majority of people (85 percent) has an Internet connection. The greater part of these connections are broadband (80 percent), making the Netherlands one of the world's leading countries on broadband penetration. Emailing, chatting, searching for information, reading the news, sharing files, buying and selling goods and services, and banking are the most frequent activities on the Internet.[287]

The presence of ICT facilities in homes of families with teenagers aged between 13 and 18 years has increased in recent years. At the end of 2005, virtually every family had at least one computer. Additionally, almost every family had an Internet connection (of which 94 percent were broadband connections). Young people use the Internet primarily for communication and entertainment. Almost all young people now own a mobile telephone. They mainly use their phone to make calls or to send SMS messages.[288]

---

[285] ECP.NL originally stood for Electronic Commerce Platform Netherlands. It does not cover the Internet safety work and focus anymore, so ECP.NL is now only used as a brand and to indicate the pay off platform for eNetherlands.

[286] Centraal Bureau voor de Statistiek (CBS - Central Statistics Bureau), "Bevolking; kerncijfers (Population; key figures)," October 24, 2007, http://statline.cbs.nl/StatWeb/Table.asp?STB=T&LA=nl&DM=SLNL&PA=37296ned&D1=a&D2=0,10,20,30,40,50,(l-1)-l&HDR=G1.

[287] "Bevolking; kerncijfers".

[288] Duimer, Marion and Jos de Haan, "Nieuwe links in het gezin. De digitale leefwereld van tieners en de rol van hun ouders (New links in the family: The digital world of teenagers and the role of their parents)," Sociaal en Cultureel Planbureau (SCP - Social and Cultural Planning Office), April 11, 2007, http://www.scp.nl/boeken/9789037702873.shtml.

Internet Safety

With its high Internet penetration, the Netherlands has its share of online problems, much the same as experienced in other countries, such as: spam, viruses, online bullying, phishing, hacking, and inappropriate content. Thus, there is an increased need for education and information about the digital world for teachers, parents, politicians, government, and SMEs.

The computers teenagers use most frequently at home usually have an anti-virus program installed, as well as other protection against unwanted intrusions, such as firewall, anti-spyware and software to protect against pop-ups. However, filters to block websites with sexual or violent content are only installed on one in five computers. Although, only a minority of young people in the Netherlands, have stated they are troubled by sexual or violent images. They are most bothered by advertising, pop-ups and spam received via email.[289]

Primary Current Issues

Currently in the Netherlands the main issues related to Internet safety are: online gaming issues, privacy concerns, filtering harmful content, and cybercrime. Cybercrime is defined as organized computer crime such as phishing and identity theft. Recently, various banks have reported phishing incidents. As of yet cybercrime is not so noticeable to people, but it is very severe, and it is estimated that the amount of incidents will increase and will be more professional in time.[290] In response, the Dutch cabinet has made plans and reserved budgets to fight cybercrime.[291]

Activities of Public and Private Bodies

In the Netherlands, there are many organizations working on the issue of safer use of the Internet. The various organizations deal with different target groups, such as elderly people, youngsters, SMEs or consumers. Among these are: major Internet providers, who are aware of their responsibility towards society and want to be of assistance, but also use Safer Internet as a marketing tool; the Dutch consumer organization; and several foundations (such as the Netherlands Institute for the Classification of Audiovisual Media (NICAM) and the Children's Consumer Organization (De Kinderconsument)). Industry has also launched its own specific campaigns. For instance, the Dutch Association of Banks (NVB) initiated a campaign about safe Internet banking. Additionally, NVB launched a

[289] Nieuwe links in het gezin. De digitale leefwereld van tieners en de rol van hun ouders.
[290] Experts like OPTA (the post and electronic communications regulator), KLPD (the Dutch police) and Govcert (the Computer Emergency Response Team of the Dutch government) think there will be more incidents in the future.
[291] Ministry of Justice, "Cybercrime," http://www.justitie.nl/onderwerpen/criminaliteit/cybercrime/, (in Dutch only).

mass multimedia campaign with TV commercials and various information materials, entitled “drie keer kloppen” (knock three times).

Also, the Dutch government sponsors different activities, such as the very important Digibewust (Digitally Aware). The objectives of this program, in which private parties are participating, are to establish a warning service[292] for Internet security incidents, and to develop a safer Internet certificate for primary schools.

With the launch of the Digibewust initiative, which was initiated in early 2006 and became a National Awareness Node at the end of 2006, government (the Ministry of Economic Affairs) and industry now combine finances and ideas for broad educational activities to promote safe use of the Internet. Also, different non-profit foundations (including the aforementioned) have been and still are combining forces and giving a boost to safe Internet use in the Netherlands.

Awareness Campaigns

In 2005, in order to further boost safe Internet use awareness, the Dutch government reserved money for three years from 2006 to 2008.[293] At the same time, different private companies (such as KPN (a Dutch telephone operator) and Microsoft) integrated their campaigns into Digibewust to ensure maximum synergy and optimal results. On Safer Internet Day 2006, the Dutch Awareness Node (from the EU Insafe network) and Surf op Safe (Safe Surfing) organized a variety of activities. In addition, some private companies, along with a number of public bodies, and the Ministry of Economic Affairs launched the significant Digibewust campaign to encourage the use of Internet and other technologies, while at the same time raising the awareness of the possible risks and the precautions one should take to use the Internet safely. At the end of 2006, Digibewust became the National Awareness Node.

The awareness campaigns that have been initiated thus far by Digibewust have resulted in the following:

- A website (in Dutch), www.digibewust.nl, which is the basis for several hundreds of pages of Internet safety and related information focused on individual target groups (parents, educators, consumers, SMEs, etc.) has been created. The site attracts some 5,000 visitors a day and contains checklists, course materials, publications and links to more information provided by other organizations.
- Various awareness materials, such as brochures and leaflets, aimed at a range of target groups, have been developed. These vary from a brochure that

[292] The Dutch version of the website is at: http://www.waarschuwingsdienst.nl/ and the English version can be found at: http://www.waarschuwingsdienst.nl/render.html?cid=106.
[293] Information on this 3-year commitment can be found at: www.digibewust.nl. This program is a proposal agreement between ECP.NL and the Ministry of Economic Affairs.

gives overall information about different internet activities, to a box with specific information for schools.

- A password campaign for teenagers has been launched in order to make them more careful with their passwords and to give them tips on how to make safe, hard-to-guess passwords. The campaign used TV commercials (broadcasted by TMF, a popular music channel for youngsters) and postcards. More than 70,000 downloads and more then 225,000 postcards (spread via libraries and high schools) found their way to the teenagers.
- A youth advisory board was set up. Twelve youngsters (aged 12 to 18) advised Digibewust and the Dutch government on what topics they would like to learn more about, and by which means of communication this information could be most effectively conveyed to them.
- An online game for children aged 8 to 14, Gebouw 13 (Building 13), was developed to let them get acquainted with the advantages and the risks of the Internet. This game was promoted by popular online children websites and MSN.com. Approximately 100,000 children have played the game.
- The celebration of the Safer Internet Day on February 6, 2007 was an important opportunity to get more attention for safe use of the Internet. Digibewust combined forces with the Child Phone (Kindertelefoon) telephone helpline for children. The presence of Princess Maxima at the Safer Internet Day events was very helpful for getting press coverage. On the Safer Internet Day 2008 the main theme will be online gaming. Prior to this, a national debate with politicians, youth, parents, students, industry, government, and other important stakeholders will be organized.
- Various events have been organized, such as: the Social Networking Event[294], which will take place on November 27, 2007, and the event Digibewust coordinated together with the Social and Cultural Planning Office of the Netherlands (Sociaal en cultureel planbureau - SCP) about use of the Internet and ICT in homes.
- For SMEs, Digibewust developed an online test, the Digibarometer. By taking this test SMEs can see how they score on digital safety and how they can improve their situation. SMEs often think that their digital safety is adequate, but still a lot of companies are victim of digital incidents, such as virus infections or information theft.
- On International System Administrator Appreciation Day on July 27, 2007, Digibewust called on businesses to acknowledge the work of system administrators. Via a special website, colleagues could nominate their system administrators to win prizes, or could send them emails stating how much their work was appreciated.
- Digibewust supported other awareness campaigns, such as “Internet SOA”[295], that educate teenagers about what could go wrong on the Internet

[294] http://www.digibewust.nl/news/item/Social_Networking_Event/89 that took place on March 15 2007; for more information please visit http://www.scp.nl/publicaties/persberichten/9789037702873.shtml

[295] See: http://www.internetsoa.nl/page.php. SOA stands for STD (sexually transmitted diseases).

and what the consequences could be. This campaign utilized TV commercials, posters at schools and a website.

Other Education and Awareness Organizations

In the Netherlands, different public and private parties are working on the issue of safer use of the Internet. Each organization targets a different group like youngsters, parents, senior citizens, SMEs or consumers. The main parties and their activities are described below.

De Kinderconsument

The De Kinderconsument (the Children's Consumer Organization)[296] endeavors to protect children and teenagers in the multimedia age. It does this by educating parents, school staff, police forces, and government.

Mijn Kind Online

The Mijn Kind Online (My Child Online) foundation is an independent information and advisory centre on youth and (new) media that focuses on providing parents with further insight on the possibilities and sensible usage of new media. To this end, the foundation has set up two websites,[297] one for parents and one for teachers. Mijn Kind Online is a joint initiative of KPN and 'Ouders Online' (Parents Online).[298]

Kennisnet ICT op school

The 'Kennisnet Ict op school' (network of ICT knowledge in the school) foundation[299] is the public IT support organization for the education sector. It looks after the interests of the Dutch education sector in the field of ICT; aids with making choices on IT-products and services; and supplies educational services and products to innovate learning and teaching.

The foundation is also the expertise centre when it comes to IT and education. There are two main activities of the foundation: provision of service (Kennisnet),[300] and protection of interests (ICT op school).[301]

[296] http://www.kinderconsument.nl
[297] "My Child Online" is at: http://www.mijnkindonline.nl/ and "My Student Online" can be found at: http://www.planet.nl/planet/show/id=1096809/sc=73d234.
[298] www.oudersonline.nl
[299] For information in Dutch, see http://www.kennisnetictopschool.nl/. The English version of the site can be accessed at: http://www.kennisnetictopschool.nl/international.
[300] www.kennisnet.nl
[301] www.ictopschool.net

Technika 10

Technika 10 Nederland[302] is an expert in the area of children and technology/IT, which focuses particularly on girls. For twenty years Technika 10 Nederland has organized technology activities for children 4 to 15 years old. The organization gets children acquainted with technology and IT in a playful manner and develops educational materials and trains adults who work with children and youngsters. Technika 10 Nederland is also a co-developer of the Ministry of Economic Affairs teaching package 'Diploma Veilig Internet' (Safe Internet Diploma).[303]

Meldpunt Kinderporno op Internet (Meldpunt)

Meldpunt Kinderporno op Internet (Hotline for Child Pornography on the Internet)[304] is an independent private foundation which aims to contribute to a reduction of child pornography on the Internet.

Meldpunt limits itself to reports on child pornography on the public areas of the Internet. Reports concerning other illegal matter on the Internet and reports regarding child pornography off the Internet do not fall under its mandate. In addition to the receiving and processing of reports by Internet users, Meldpunt also gives information to parents, children and teachers about safe use of the Internet via the website www.surfsafe.nl. Also, a website for young people, www.helpwanted.nl, is a part of Meldpunt; this is a reporting site where youngsters can (anonymously) report when they are being bullied or abused on the Internet.

Stichting Kinderen, Opvoeding, Educatie en Internet (Stichting K.O.E.I.)

The independent K.O.E.I. foundation (Foundation of Children, Education and the Internet)[305] aims to look after the interests of children ages 0 to 18 with regard to Internet skills and resistance to online dangers. The foundation tries to reach these goals by:

- providing insight to parents and teachers about the Internet usage and "virtual" experience of children and young people;
- developing expertise of the Internet and online education for parents and teachers;
- making resources available to parents, teachers and children to be able to improve their Internet capabilities;
- establishing relationships with other organizations and companies, which support the foundation and its goals; and

[302] www.technika10.nl
[303] http://www.iksurfveilig.nl/
[304] The Dutch site can be found at: http://www.meldpunt-kinderporno.nl/. The English version is available at: http://www.meldpunt-kinderporno.nl/en/.
[305] www.stichtingkoei.nl

- promoting an array of activities which reflect the Internet interests of children and young people as independent Internet users.

PEGI Online

The Pan European Game Information (PEGI) system[306] lets parents determine which computer games are suitable for their children. With a specific age classification, which makes use of special symbols, the PEGI system offers a detailed description of content. As an addition to the PEGI system, PEGI Online[307] was developed to protect children from inappropriate online game content. If an online game meets the requirements of the PEGI Online Safety Code, the game provider is allowed to use the PEGI Online Logo. PEGI is funded by the European "Safer Internet" Program.

In the Netherlands, NICAM is the administrator of the PEGI system. NICAM is running 'Kijkwijzer' (Look Indicator)[308], the national uniform system for the classification of television, cinema film, DVD, and mobile content.

[306] http://www.pegi.info/en/index/
[307] http://www.pegionline.eu/en/index/
[308] http://www.kijkwijzer.nl/

Child- and Teen-Oriented Websites in the Netherlands

Awareness
Digibewust (Digitally Aware) - www.digibewust.nl
Waarschuwingsdienst (the Dutch National Alerting Service) - www.waarschuwingsdienst.nl
SIF (Safer Internet Foundation) - www.sif.nl
ICT op School (ICT for School) - www.ictopschool.net
Kennisnet ICT op School (Provision of ICT Services for Schools) - www.kennisnet.nl
Be Safe Online - www.besafeonline.org
Surf Safe - www.surfsafe.nl
School en veiligheid (School and Safety) - www.schoolenveiligheid.nl
MSN veilig online (MSN Safety Online) - http://services.nl.msn.com/Security/
Mijn Kind Online (My Child Online) - www.mijnkindonline.nl
Mijn Leerling Online (My Student Online) - http://www.planet.nl/planet/show/id=1096809/sc=73d234
Pestweb (website about online bullying) - http://www.pestweb.nl/aps/pestweb
www.pesten.nl

Education
Technika 10's Internet Oké (Internet OK) - http://www.technika10.nl/meiden/internetok.htm
Muisje Max (Mouse Max) - www.rsi-centrum.nl/doc/muisjemax
Zap Game - http://www.e-linq.nl/zap/nl/game.html
Webkwestie (Web Quest - a site that teaches children how to search on the Internet) - www.webkwestie.nl/
Webdetective - www.webdetective.nl/
Digibewust Gebouw 13 (Digitally Aware Building 13) - www.gebouw13.nl

Hotlines
Meldpunt Discriminatie (Dutch Complaints Bureau for Discrimination on the Internet) - www.meldpunt.nl
Meldpunt Kinderporno (Hotline for Child Pornography on the Internet) - www.meldpunt-kinderporno.nl
Meldpunt ICT-veiligheid (Hotline for ICT safety) - www.waarschuwingsdienst.nl/ Spamklacht (Opta) (Complaining against Spam) - www.spamklacht.nl

Research
Filtertest (test for filtering) - http://www.ictopschool.net/infrastructuur/publicaties/uitgaven/filter/conclusies.html
SCP Nieuwe links in het gezin (Social and Cultural planning office: new links in the family) - www.scp.nl/boeken/9789037702873.shtml

Magazines
Vives (a booklet that educates teachers about the latest ICT trends) - www.vives.nl
Computers op School (Computers at school) - www.computersopschool.nl/

Conclusion

The Internet has profoundly changed the way we communicate and is here to stay. It can empower us and gives us the ability to share ideas and information on a worldwide basis. But if Internet use is unchecked, it can also cause a lot of damage.

The Netherlands has, with its high Internet penetration, its share of online problems, like spam, viruses, online bullying, phishing, privacy and ID management issues, lack of media literacy, hacking, and inappropriate content.

An array of statistics shows that Internet safety is not only a matter of technical measures. As a matter of fact, almost all people and industry adopt the most common technical security measures. The fact that this does not lead to a safer Internet environment is because of the 'human factor': people know there are risks and implement the standard security measures, but they simply do not know what to do next, never check again or just do not know how to check, are careless, or they put too much trust in their service providers or children.

Thus, awareness raising is essential. First of all, consumers must not rely completely on their service provider and the installed security software, because there is often a lack of quality. Secondly, installing software is just the first step; the second step is acting in a safe way in the online world. Therefore one needs to know what the risks are and how to act ethically, correctly and safely.

Chapter VIII:
Belgium and Europe

by Rudi Vansnick, President, Internet Society Belgium and ICT consultant, Belgium

Introduction

Belgium, being one of the most widely cabled countries in Europe, has still not attained the Internet penetration one could expect from a country with good infrastructure. Getting safe and secure access to the Internet is, in most cases, well covered by ISPs. Nevertheless, numerous complaints have been posted on forums, especially with regard to harmful content for children, as well as for adults.

Belgium was also in the spotlight several years ago with the Dutroux paedophile case[309], which is still being debated in the courts. Cases like this get the full attention of politicians and media, as well as of all concerned adults.

At the European level, a safer Internet project, which includes an international project named “Insafe” covering issues such as Safe Internet for Children, has been launched by the European Commission.

Belgian Projects

Saferinternet.be

Saferinternet.be is a project under the umbrella of the EU project Insafe[310]. The primary goal of this project is to raise awareness for Belgian minors on how to avoid harmful and illegal content online. A special website was developed and gives some samples and blogs about an array of relevant topics such as safe chatting and legal downloading. The website also provides information and links on various child safety organizations in Belgium.

eID - the Belgian Electronic Identity Card

In 2005, the Belgian Secretary of State launched a project called “Safe Chat”, which uses the e-ID[311]. At the age of 12, children get an e-ID reader for free along with their electronic identity card. Some chat servers have been configured to use the e-ID as an access control system for young people using their chat rooms.

[309] Information on this case can be found at:
http://www.crimelibrary.com/serial_killers/predators/dutroux/evil_1.html.
[310] http://www.saferinternet.org/ww/en/pub/insafe/index.htm
[311] http://www.eid.belgium.be/

In theory, this is a good initiative. However as it is common for children to try to surpass the hurdles set to protect them as they do not like to be controlled, it is likely that online offenders know how to manipulate the control system, showing that there is still a lot of work to be done.

Action Innocence

Action Innocence[312], is an NGO that was founded in November 1999 by Mrs. Valerie Wertheimer in Geneva. Subsequently, in 2003, the Belgian chapter[313] started its activities. The goal of the organization is to ensure a safe Internet environment for children and youngsters. It does this mainly through awareness initiatives.

Internet Society Belgium - Internet Ombudsdienst

Internet Ombudsdienst[314], which was launched in early 2005 by Internet Society Belgium[315], was the first ombudsman service offered to the Internet user. In response to numerous calls for help, the service was deployed to deal with specific Internet concerns such as fraudulent transactions on the Internet, spam and other email complaints. Later, harmful content was added to the list of issues covered.

Some Thoughts on How to Improve the Situation

Protecting children from accessing harmful or illegal content is only possible if parents are able to effectively use the appropriate technical solutions. The first step is good communication between children and their parents. In many cases we see that child victims are from social environments where knowledge and awareness of the dangers are non-existent. It seems as though getting tools and technical solutions to those parents is even more difficult than children accessing harmful and illegal content.

Knowing this, it is very clear that other actions should be considered in order to make every parent, or any other person having the responsibility to protect children, aware of the possible danger while having access to the World Wide Web. The task is not fulfilled by just putting banners, buttons and information on a web page.

[312] http://www.actioninnocence.org/. Information on this organization can be found in English at: http://www.genevahumanitarianforum.org/record.php?view=list&type=12&sortColumn=sName&sortDir=ASC&pageSize=10&id=796&PHPSESSID=8fec474661e7b45692e8c17b6b4b15cd

[313] The French website can be accessed at: http://www.actioninnocence.org/belgique/index.asp?navig=15 and the Flemish website is at: http://www.actioninnocence.org/belgie/index.asp?navig=15

[314] Information in English on this program is available at: http://www.isoc.be/safeinternet/indexGB.htm

[315] http://www.isoc.be/news.php?sect=4

As an example, the *Safe Chat* project has proven that children will try to avoid being controlled and will use the non-safe access to that chat room. Moreover, the offender will also try to get access to the *Safe Chat* environment.

Schools have the possibility to install special software such as some kind of electronic 'babysitting'. Net Nanny and Cyberpatrol are good examples. However no standard definition of usage has yet been done by government or by any official body.

Statistics

- The statistics (2006) on the Belgian government Statbel site show that 54 % of the Belgian households have access to the Internet, same figure as we see for the global EU (15 member states).[316]
- In total about 2.5 million Internet connections exist in Belgium where 2.05 million are private (home use) Internet connections.[317]
- Belgium has about 4.2 million Internet users
- Broadband penetration in some areas is more than 90%. The cost for a broadband connection is very high, one of the highest in Europe. Despite the presence of a very strong cable network, there are not enough providers to compete and thus prices do not decrease.[318]

Kids on the Internet in Belgium

In just a few years young people have discovered the many flavours of the Internet. The usage of this medium started to increase at the same time as dangers against harmful and illegal content rose.

Use of internet by age.

Ages	use in %
9 to 10 years	84 %
11 to 12 years	87 %
13 to 14 years	95 %
15 to 17 years	96 %
18 years	97 %

Source: Study 2006 OIVO-CRIOC.

316 Information available on the Belgian government website (Economical affairs) http://statbel.fgov.be/figures/d75_nl.asp#6

317 See point 1 above.

318 Data gathered from ISPA website (Internet Service Providers Association) http://www.ispa.be/default.aspx?sitelang=english

Where do they use the Internet?

Location	%
At home	93 %
At school	25 %
At a friend's home	19 %
In family	10 %
In a cybercafé	3 %
Somewhere else	2 %

Source: Study 2006 OIVO-CRIOC.

Education and Awareness Efforts

Many efforts are taken by the European Commission, especially the Safer Internet Project. As part of a coherent approach by the European Union, this project aims to promote safer use of the Internet and new online technologies, particularly for children, and to fight against illegal content and content unwanted by the end-user.

European Union (EU) Projects

The European Commission's "Safer Internet Plan"[319] provides funding to EU countries to deal with illegal and harmful content, and supports EU member states' regulations and decisions. It encourages self-regulation and supports a European network of safer Internet awareness centres. It ran for an initial period between 1999 and 2002 and in May 2003 was extended until December 31, 2004, with a budget increase of 13.3 million Euro. It has since been renewed from January 2005 to December 2009.

Safer Internet Plus Program

The "Safer Internet *plus*"[320] program aims to promote safer use of the Internet and new online technologies, particularly for children, and to fight against illegal and unwanted content, as part of a coherent approach by the EU. The program has four main actions: fighting against illegal content; tackling unwanted and harmful content; promoting a safer environment; and awareness-raising.

The Safer Internet *plus* program covers new online technologies, including mobile and broadband content; online games; peer-to-peer file transfer; and all forms of real-time communications, such as chat rooms and instant messaging,

[319] http://ec.europa.eu/information_society/activities/sip/index_en.htm
[320] http://ec.europa.eu/information_society/activities/sip/programme/index_en.htm

primarily with the aim of improving the protection of minors. Action will be taken to ensure that a broader range of illegal and harmful content, in addition to worrisome conduct, including racism and violence, is covered.

Eurobarometer

In a pan-European qualitative study[321], covering 29 European countries (the 27 member states and Norway and Iceland), children ages 9 to 10 and 12 to 14 were interviewed about their use of online technologies, their online behavior, and how they perceive and deal with risks. The study was commissioned by the Directorate-General for Information Society and Media (DGINFSO) and was conducted by OPTEM and its European partners.[322] The results of the study are to be used to contribute to the design of the Safer Internet Program and to increase the effectiveness of awareness building actions.[323]

Insafe

Insafe[324] is a network of national nodes which coordinates Internet safety awareness initiatives in Europe. The network was established and is co-financed within the framework of the European Commission's Safer Internet *plus* Program.[325]

The objective of the Insafe network is to empower citizens to use the Internet and other online technologies confidently, safely and effectively. The network advocates shared responsibility by government, educators, parents, media, industry and other relevant actors for the protection of the rights and needs of citizens, in particular youth. Insafe partners work closely together to share best practices, useful information and resources. Also, with the goal of empowering people to bridge the digital divide between home and school and between generations, the network interacts with industry, schools and families.[326]

Insafe partners examine and address emerging trends, at the same time as seeking to underline the idea of the web as a good place to learn. They make an effort to raise awareness about how harmful or illegal content and services can be reported. Through close cooperation between partners and other actors,

[321] A summary of the study can be found at: http://ec.europa.eu/information_society/activities/sip/docs/eurobarometer/qualitative_study_2007/summary_report_en.pdf. For a European Commission press release on the study, see: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/07/1227&format=HTML&aged=0&language=EN&guiLanguage=en.
[322] DGINFSO, "Eurobarometer on Safer Internet for Children: qualitative study 2007," http://ec.europa.eu/information_society/activities/sip/eurobarometer/index_en.htm
[323] Ibid.
[324] http://www.saferinternet.org/ww/en/pub/insafe/index.htm
[325] http://www.saferinternet.org/ww/en/pub/insafe/about.htm
[326] Ibid.

Insafe endeavors to raise Internet safety awareness standards and support the development of media literacy for all.[327]

Safer internet shielding benchmark (SIP-Bench):

The Safer Internet Plan Benchmark aims to:

- improve awareness of solutions and promote best practice
- provide guidance to parents / educators
- steer software vendors and services providers
- make a clear distinction between:
  - Age 6-10 years
  - Age 11-14 years
  - Age 15-16 years

The 2006 benchmark involved 110 parents and teachers speaking nine different languages. In addition, a lab was built with its own web servers, mail servers, file servers and chat servers to test all 30 tools in exactly the same circumstances. To test the effectiveness of the tools against a variety of content, 5000 test cases were compiled and classified using criteria that simulated the concerns of an average European parent.

The 2006 edition of the benchmark shows that today's filtering tools are capable of filtering potentially harmful content without seriously degrading the Internet experience of youngsters. Yet, the industry should aim at filtering not only the obvious harmful content but take the considerations of European parents and teachers into account. Indeed, tests show that filtering content on-the-fly in a consumer context remains a challenge.

The benchmark indeed shows that tools performed well in filtering content from sites with millions of hits per day, containing obvious content (read: porn) expressed in a common language (read: English). In fact, we identified 12 products which made a wrong filtering decision in less than half the cases and there was one tool that was wrong in only 1 out of 16. However, when trying to filter less obvious but equally harmful content, it was found that none of the tools were capable of filtering adequately. All products, without exception, got it wrong in more than one quarter of the test cases.

Source : SIP Benchproject

Conclusion

There is widespread support for some form of standardization for internet filtering tools among consumer organizations and other organizations involved in internet safety issues in Europe.

[327] Ibid.

Chapter IX:
Mexico

by Marie-Claire Hernandez, President, Family & Society, Mexico
and
Armando Novoa, Director, Navega Protegido, Mexico

Introduction

In 2004, Family & Society, a civil association based in Mexico City, became aware of the need to create a safer online environment in Mexico, especially for teenagers and children, as a result of the detection of cases of children and teenagers with addiction to Internet pornography. Thus, it launched a project, which was divided into four different areas: education and prevention; therapy for victims of addiction to Internet pornography; legislation and public policies; and technology to make the Internet a safe and enjoyable experience.

Initially, public speaking and certain tools, such as leaflets, helped raise awareness, but it was the relationships developed by Family & Society with British Telecom (BT) and the Children's Charities' Coalition on Internet Safety (CHIS)[328] in the UK, and subsequently with the Internet Content Rating Association (ICRA)[329] and the Family Online Safety Institute (FOSI)[330] in Washington, that were instrumental in strengthening the impetus for the project.

In April 2006, members of Family & Society met with Nick Truman (Head of Internet Security at BT) and John Carr (Technology Advisor at the Children's Charity - NCH[331]) in London. In June 2006, Family & Society visited ICRA in Washington for a meeting on online safety with similar civil society institutions based in Washington. In November 2006, a private seminar on technological tools and safe practices was given by ICRA at Telmex, the leading telecommunications company in Mexico. As a result of this event, Telmex' committed to joining ICRA. When ICRA revamped itself as FOSI, Telmex participated in the launch and became a founding member in Washington, DC on February 13, 2007.[332]

[328] http://www.nch.org.uk/information/index.php?i=209
[329] http://www.fosi.org/icra/
[330] http://www.fosi.org/
[331] http://www.nch.org.uk/
[332] Information on Telmex's involvement in FOSI can be found at: http://www.fosi.org/members/.

Mexico City Conference

After becoming a member of FOSI, Telmex[333], along with FOSI, Family & Society, and Navega Protegido en Internet (Safe Internet Browsing)[334], decided to host a conference[335] in Mexico City on June 13, 2007 to discuss the aforementioned Family & Society project and its four components. The main focus of the conference was the major issues young people and families are facing on the Internet in Mexico. The most important achievement of this conference was that it served to establish consensus on a number of online safety issues.

It also brought to light several other valuable initiatives that others had been working on in the field of online safety, such as those of the Mexican Internet Association (AMIPCI)[336], the National Institute for the Penal Sciences (INACIPE)[337], and Navega Protegido en Internet (an industry initiative which promotes safe surfing through educational tools and literature).

Navega Protegido en Internet has established real contact with Internet users in Mexico through their advisory services and their website, www.navegaprotegido.org.mx, and as a result has gained insight into the problems Internet users encounter. The site was launched in November 2005, and in the first eighteen months Navega Protegido answered over 5,000 questions on subjects relating to basic security (virus, firewall, etc.), personal security (spam, e-bank, etc.) and family safety online (child protection, content filtering, etc.).

Navega Protegido has also organized two major conferences, the first on online identity protection, phishing and financial e-frauds, and the second on family online safety. It has produced thousands of free printed materials distributed during the conferences, as well as in 30 seminars on web security held during 2006.

At present, all these organizations, together with the different sectors in Mexico, including industry, civil society, psychologists, educators, and government, are working hard to implement the conclusions and commitments from the Mexico City conference in order to reach a national consensus on online safety and promote a safer online experience.

With the participation of outstanding specialists and representatives from more than 50 private and public companies and institutions, both from Mexico and abroad, the work of the four roundtables (on psychology, legislation, education,

[333] http://www.telmex.com/mx/
[334] http://www.navegaprotegido.org.mx/
[335] http://www.telmex.com/mx/esto/seguridadenlinealist.html
[336] http://www.amipci.org.mx/
[337] http://www.inacipe.gob.mx/

and technology) at the June 13 conference resulted in the conclusions and commitments[338] described below.

Roundtable on Psychology: "A New Line of Therapy"

The aim of this roundtable was to evaluate the risk factors of addiction to Internet pornography among children and teenagers, as well as to identify the characteristics of child and teenage victims of Internet pornography addiction, and to outline suitable therapy for victims.

With regard to these matters, the panelists concurred on the following action items:

- urgent need to create a culture of responsibility with set norms and rules mainly among parents regarding the use of the Internet;
- development of research plans to study risk factors, consequences, implications, and treatment that would allow for effective intervention in cases of addiction;
- design of instruments and mechanisms of evaluation for timely diagnosis and prognosis for each case;
- creation of Internet tools, such as a hotline, for increasing awareness about the problem of addiction to harmful content, which, while guaranteeing anonymity for children and teenagers with this problem, would provide them with professional psychological assistance;
- launching of rehabilitation programs with networks of support for the family;
- development of a directory of multidisciplinary specialists;
- establishment of networks between institutions to promote training and interaction among specialists; and
- creation of a national association for undertaking the proposed projects in therapy.

Roundtable on Legislation: "Legal Framework and Public Policy for Online Safety"

The panelists analyzed the national legal framework and public policy regarding online safety and reviewed some related international experiences. The conclusions on these matters are as follows:

- The strengthening of the legal framework to help minors browse on the Internet safely should stem from the recognition that joint responsibility of the government, families, and schools is necessary.
- Industry self-regulation may not exist without the corresponding legislation.
- Censure measures are legally justifiable with regard to protection of minors.

[338] Information on the conclusions and commitments as detailed in this chapter can be found, in Spanish only, at: http://www.telmex.com/mx/esto/salaPrensa_ComPrensa2007_071407.html.

- Greater promotion of applicable laws in this matter (i.e. Articles 200, 202-205, and 208 of the Mexican Federal Criminal Law) and espousal of a law-abiding culture are crucial.
- Criminal laws that protect minors shall be adapted to the actual technological context.
- The authorities responsible for the enforcement of applicable laws regarding minors shall be actively involved in the work performed by civil society and Internet safety companies, and promote modernization of the legal framework.
- There was a proposal for an Inter-secretarial Commission to be established to ensure that the Executive Power could actively participate in the updating of the legal framework for the protection of minors.
- A specialized Prosecution Office for cybercrime was proposed.

Roundtable on Education, Communication and Prevention: "Online Safety Campaign"

At this Roundtable, the risk factors surrounding addiction to Internet pornography among children and teenagers were identified and evaluated in order to determine the most suitable educational strategies for teaching online safety. The main agreements and commitments were the following:

- It is necessary to establish an educational strategy that allows the use and benefits of the Internet, while protecting against the risks.
- Every educational and prevention strategy should take into account the fundamental role of the State and the family as educators, each according to their specific area of responsibility.
- The State should encourage the technological literacy of parents and teachers, so they in turn may promote correct criteria in the use of technological tools.
- The creation of an educational "get safe online" campaign which involves government, industry, the community, schools, and families was proposed.
- The educational campaign should promote the values of the new cybernaut generations, as well as provide information about the existence of the dangers online, methods of self-protection, ways of combating negative effects and damages, where and how to report crime, and how to ask for help.

Roundtable on Technology: "Technological Tools for Online Safety"

The aim of this roundtable was to agree on mechanisms that would ensure that all users have the technological tools that result in better and greater control while browsing the Internet, particularly regarding protection against inappropriate content for minors. In this regard, the panelists proposed the following:

- The industry should find the best ways to self-regulate.
- Industry needs to commit to developing user-centered tools and technology.
- Promotion and education of the existing control and safety tools, for all communication media, are necessary.

- A Mexican Association of Internet Service Providers (ISPs) should be established.
- Promotion of self-classification of websites, starting with government sites, should be carried out following ICRA's international standards.
- McAfee and Symantec agreed to share and promote online safety courses, in addition to providing greater access to their security programs.
- Yahoo and Google agreed to include links on their toolbars to the Navega Protegido website, which offers educational content on online safety.
- Telmex agreed to soon introduce an online protection tool.

Conclusion

Although Mexico is relatively new to the field of online safety, and there is much still to be done, we hope to take the lead in encouraging other Spanish speaking countries to become involved in the projects of online safety promoted by FOSI. The successful conference hosted in Mexico City encouraged the Spanish to have a similar event on September 26, 2007 in Madrid and there are now talks of Brazil following suit.

Abbreviations List

General

EU - European Union
FOSI - Family Online Safety Institute
FTP - File Transfer Protocol
HTTP - Hypertext Transfer Protocol
ICH - Internet Content Host
ICRA - Internet Content Rating Association
ICT - Internet and Communications Technology
INHOPE - Internet Hotline Providers Association
ISP - Internet Service Provider
NGO - Non-Governmental Organization
OECD - Organization for Economic Co-operation and Development
PC - Personal Computer
PEGI - Pan European Game Information (System)
SIAP - Safer Internet Action Plan
SME - Small or Medium-sized Enterprise
SMS - Short Message Service (text messaging)
URL - Uniform Resource Locator (web address)
VoIP - Voice over Internet Protocol

Chapter I - United States

ACLU – American Civil Liberties Union
APIs - Application Programming Interfaces
BSPs - Broadband Service Providers
CDA - Communications Decency Act
CIPA - Children's Internet Protection Act
COPA - Child Online Protection Act
COPPA - Children's Online Privacy Protection Act
DOJ - Department of Justice
FBI - Federal Bureau of Investigation
FCC - Federal Communications Commission
FTC - Federal Trade Commission
IM – Instant Message
NCTA - National Cable & Telecommunications Association
RIAA - Recording Industry Association of America
SAFER NET Act - Safeguarding America's Families by Enhancing and Reorganizing New and Efficient Technologies Act

Chapter II - United Kingdom

ACPO - Association of Chief Police Officers
BECTA - British Education Communication Technology Agency

BT - British Telecom
CEOP - Child Exploitation and Online Protection Centre
CHIS - Children's Charities' Coalition for Internet Safety
CSPs - Content Service Providers
ECPAT - End Child Prostitution, Child Pornography and the Trafficking of Children for Sexual Purposes
ITFCPI - Internet Task Force for Child Protection on the Internet
IWF - Internet Watch Foundation
NCH – the Children's Charity
NCVCCO - National Council of Voluntary Child Care Organizations
NSPCC - National Society for Prevention of Cruelty to Children
Ofcom - Office of Communications
POLIT - Paedophile Online Investigation Team
SOCA - Serious Organised Crimes Agency
SQA - Scottish Qualifications Authority
VGT - Virtual Global Taskforce

Chapter III - Germany

DSIN - Germany Securely on the Net (Deutschland sicher im Netz)
eco - Federation of the German Internet Economy (an Internet Service Providers Association)
FSM - Impartial Self-checking Multimedia Service Tenderer (Freiwillige Selbstkontrolle Multimedia-Diensteanbieter)
JMStV - Interstate Treaty for the Protection of Human Dignity and the Protection of Minors in the Media (Jugendmedienschutz-Staatsvertrag)
JuSchG - Youth Protection Act (Jugendschutzgesetz)
KJM - Commission for the Protection of Minors in the Media (Kommission für Jugendmedienschutz)

Chapter IV - Australia

ABS - Australian Bureau of Statistics
ACMA - Australian Communications and Media Authority
AFP - Australian Federal Police
CSIRO - Commonwealth Scientific and Industrial Research Organization
DCITA - Department of Communications, Information Technology and the Arts
IIA - Internet Industry Association
MMS - Multimedia Messaging Service
OECD - Organization for Economic Co-operation and Development
OCSET - Online Child Sex Exploitation Team
PAFO - Protecting Australian Families Online (initiative)
RC - Refused Classification
RMIT - Australian University

Chapter V - Canada

CCAICE - Canadian Coalition Against Internet Child Exploitation
CRTC - Canadian Radio-Television and Telecommunications Commission
DPSEPC- Department of Public Safety and Emergency Preparedness Canada
KINSA - Kids' Internet Safety Alliance
MNet - Media Awareness Network
OPHEA - Ontario Physical and Health Education Association
PSC - Public Safety Canada
RCMP - Royal Canadian Mounted Police
SOLOS - Safe Online Outreach Society
YTV - Youth Television (a station aimed at a child audience)

Chapter VI - Austria

ISPA - Internet Service Providers Association of Austria
PEGI - Pan European Game Information
ÖIAT - Austrian Institute for Applied Telecommunications

Chapter VII - The Netherlands

K.O.E.I. Foundation - Foundation of Children, Education and the Internet (Stichting Kinderen, Opvoeding, Educatie en Internet - Stichting K.O.E.I.)
KPN - a Dutch telephone operator
Meldpunt - Hotline for Child Pornography on the Internet (Meldpunt Kinderporno op Internet)
NICAM - Netherlands Institute for the Classification of Audiovisual Media
NVB - Dutch Association of Banks
PEGI - Pan European Game Information

Chapter VIII - Belgium and Europe

DGINFSO - Directorate-General for Information Society and Media
SIP-Bench - Safer Internet Plan Benchmark

Chapter IX - Mexico

AMIPCI - Mexican Internet Association
BT - British Telecom
CHIS - Children's Charities' Coalition on Internet Safety
INACIPE - National Institute for the Penal Sciences
NCH - Children's Charities' Coalition on Internet Safety

Family
Online Safety
Institute

The Family Online Safety Institute is an international non-profit organization that actively works to identify and promote best practices, tools and methods in the field of online safety. The organization facilitates the meeting of thought leaders in technology, policy and education, culminating in its Annual Conference. FOSI also incorporates the work and mission of the Internet Content Rating Association (ICRA), the world's leading content labeling system for the Internet, providing families with the tools they need to protect their children and ensuring continued freedom of expression for content providers. FOSI is headquartered in Washington D.C. and has additional locations in the UK, Germany and Austria. For more information, please visit www.fosi.org.

666 11th St. NW • Suite 1100 • Washington, DC 20001 • Phone: (202) 654-4228 • Facsimile: (202) 654-4236
www.fosi.org