CENTER FOR
DEMOCRACY
&
TECHNOLOGY
Working for Civil Liberties on the Internet

1634 I Street, NW Suite 1100
Washington, DC 20006
202.637.9800
fax 202.637.0968
http://www.cdt.org

Child Safety and Free Speech Issues in the 110th Congress

Updated as of February 15, 2007

I. Summary 1
II. Categories of Targeted Content 2
III. Conclusions of the Two Congressional Panels of Experts 3
IV. Ineffective, Flawed, and Unconstitutional Legislative Proposals 5
Mandatory Labeling (S. 49 & H.R. 837) 5
Deleting Online Predators Act (S. 49) 6
Burdens and Liability on Blogs and Social Networking Communities 7
Data Retention (H.R. 837) 7
Government Blacklists of Web Sites (S. 519 and H.R. 876) 8
V. Effective and Constitutional Legislative Proposals (including H.R. 1008) 9

I. Summary

Already in the new Congress, Senators and Representatives have introduced a wide range of proposals intended to protect children in the online environment. CDT strongly believes that protecting kids in the online environment is an important goal, and there are significant measures that Congress could enact that would further that goal. Many of the child protection proposals now pending in Congress, however, would *not* be effective at protecting kids, and raise serious policy and constitutional problems.

Leading panels of experts have concluded that the most effective way to protect kids online is to educate them about how to use the Internet and what types of content to avoid, and to promote the voluntary use of technology tools such as filtering software that parents can install on computers in the home. Direct attempts to regulate content on the Internet, in contrast, are seldom effective, in part because of the fact that more than half of the sexual content that Congress seeks to regulate is overseas, outside the reach of a U.S. criminal law or regulation.

Proposals that would mandate that web sites must "label" undesired content provide a clear example of an approach that would be ineffective (because of the overseas content problem and the simple fact that the web sites that are the purported target of the proposal can already be easily filtered) and would be clearly unconstitutional (under the "compelled speech" doctrine of the First Amendment). In contrast, Congress can take concrete actions to promote broad education of children about the rules and risks of using the Internet, and to educate parents about the use of filtering tools.

In this analysis, we (1) review the four main child protection categories that arise relating to the Internet; (2) summarize the core conclusions of the two panels of experts that Congress commissioned to study child protection online; (3) discuss current and past Congressional proposals that raise serious policy and/or constitutional problems; and finally (4) identify a number of valuable steps that Congress can take to help protect children online.

II. Categories of Targeted Content

It is important to differentiate between different categories of content that raise concerns about child safety online. The four basic content categories are:

Child pornography: Child pornography is among the most abhorrent types of content, either online or offline, and it is flatly illegal under existing federal and state criminal laws. Anyone who participates in the creation or distribution of child pornography (whether on- or offline) can be prosecuted, and the U.S. Department of Justice has brought a range of such charges relating to content distributed online. In addition to the blanket law against all child pornography, Congress has enacted an additional criminal provision against using the Internet to deliver child pornography to a minor. These laws have been on the books for more than ten years.

Obscenity: Similarly, the distribution of obscene material – whether online or offline – is flatly illegal under existing federal and state criminal laws, and the Department of Justice has brought successful prosecutions against online distributors of obscene material. As with child pornography, Congress has also created a second federal crime of using the Internet to deliver obscene material to a minor. These laws have also been on the books for more than ten years.

Material that is "harmful to minors": This category of content is fully legal for adults to access (e.g., "adult" material, sometimes called "pornography"), but may be illegal if distributed to minors. Because this content is lawful content, Congress' ability to prohibit access to it is strictly limited by the First Amendment. Congress has twice in the past sought to block this material on the Internet (in the Communications Decency Act and the Child Online Protection Act), but the Supreme Court and lower courts have repeatedly struck down these and similar state statutes under the First Amendment.

Child predators: A final category of concern involves adults using the Internet to contact children with the aim of preying on or molesting them. Law enforcement authorities have effectively arrested and prosecuted such predators, often using "sting" operations that use adults to pose online as sexually-interested children. Although the gravity of this crime cannot be understated, the prevalence of the risk has been greatly overstated. American children under 18 engage in 10 million or more online communications every day, and the vast, vast majority of those communications are perfectly innocuous and completely legal. Moreover, academic research indicates that the education of children about online predators is a vital approach to the problem.[1]

[1] Wolak, J. *et al.*. "Internet-initiated Sex Crimes against Minors: Implications for Prevention Based on Findings from a National Study" Journal of Adolescent Health 2004;35(5):424.e11-424.e20, available at http://www.unh.edu/ccrc/pdf/CV71.pdf.

III. Conclusions of the Two Congressional Panels of Experts

Two blue-ribbon panels established by Congress to investigate how best to protect children in the online environment concluded that the most effective way to protect kids online is to combine education with the use of filtering and other technology tools to empower parents to decide what content their children should access.

As part of the Child Online Protection Act passed in 1998 ("COPA"), Congress established the "COPA Commission" to "identify technological or other methods, if any, to help reduce access by minors to material that is harmful to minors on the Internet."[2] The Commission, which was comprised of 18 commissioners from government, industry and advocacy groups, representing a wide variety of political affiliations, evaluated and rated protective technologies based upon various factors including their effectiveness and implications for First Amendment values. The Commission issued a final report in October 2000.[3]

Wholly independent of the COPA Commission, Congress also instructed the National Academy of Sciences to undertake a study of "computer-based technologies and other approaches to the problem of the availability of pornographic material to children on the Internet."[4] More than two years in the making, the National Academy released its study – entitled "Youth, Pornography, and the Internet" – in May 2002.[5] The committee that prepared the National Academy of Science report was chaired by former U.S. Attorney General Richard Thornburgh, and was composed of a diverse group of people including individuals with expertise in constitutional law, law enforcement, libraries and library science, information retrieval and representation, developmental and social psychology, Internet and other information technologies, ethics, and education.[6] Over the course of its two years of study and analysis, the committee received extensive expert testimony, and conducted numerous meetings, plenary sessions, workshops, and site visits.[7]

Both the COPA Commission and the Thornburgh Committee reached the same two critical conclusions: (A) in light of the global nature of the Internet, criminal laws and other direct regulations of content inappropriate for minors will be ineffective, and (B) education and parental empowerment with filtering and other tools are far more effective than any criminal law.

---

[2] *See* COPA § 5(c), 47 U.S.C. § 231, note.

[3] The "Final Report of the COPA Commission," released on October 20, 2000, is available online at http://www.copacommission.org/report/.

[4] Pub. L. No. 105-314, Title IX, § 901, 112 Stat. 2991 (1998).

[5] *See* Nat'l Research Council of the Nat'l Academy of Sciences, "Youth, Pornography, and the Internet" (2002) ("Thornburgh Report"). The full report is available online at http://books.nap.edu/html/youth_internet/ (HTML form) or http://books.nap.edu/openbook/0309082749/html/index.html (PDF form).

[6] Thornburgh Report, at viii – x.

[7] *See* Thornburgh Report, at x – xi & appendix A.

The Thornburgh Committee determined that approximately three-quarters of the commercial sites offering sexually explicit material are located outside the United States,[8] rendering criminal law ineffective:

> For jurisdictional reasons, federal legislation cannot readily govern Web sites outside the United States, even though they are accessible within the United States. Because a substantial percentage of sexually explicit Web sites exist outside the United States, *even the strict enforcement of [the COPA statute] will likely have only a marginal effect on the availability of such material on the Internet in the United States.* Thus, even if the Supreme Court upholds COPA, COPA is not a panacea, illustrating the real limitations of policy and legal approaches to this issue.[9]

The Thornburgh Committee concluded that education and technology tools were the critical components of a strategy to keep children safe online:

> [T]he most important finding of the committee is that developing in children and youth an ethic of responsible choice and skills for appropriate behavior is foundational for all efforts to protect them—with respect to inappropriate sexually explicit material on the Internet as well as many other dangers on the Internet and in the physical world. Social and educational strategies are central to such development, but technology and public policy are important as well—and the three can act together to reinforce each other's value. . . .
>
> . . . .
>
> Technology-based tools, such as filters, can provide parents and other responsible adults with additional choices as to how best to fulfill their responsibilities. Though even the most enthusiastic technology vendors acknowledge that their technologies are not perfect and that supervision and education are necessary when technology fails, tools need not be perfect to be helpful . . . .[10]

And critically, the Thornburgh Report suggests that one should look beyond criminal laws for governmental and public policy actions that would help to protect children. As the report noted, "public policy can go far beyond the creation of statutory punishment for violating some approved canon of behavior."

Congress should follow the recommendations of these two blue-ribbon panels, and focus its efforts on promoting education of children about the Internet and the use of filtering tools by parents to protect their children. Attempts to regulate Internet content directly, in contrast, will be ineffective and will raise significant constitutional and policy concerns.

---

[8] *See* Thornburgh Report, at 4.

[9] Thornburgh Report, at 207 (emphasis added). *See also* Thornburgh Report, at 360 (further detailing why U.S. laws will be ineffective). The COPA Commission also recognized that overseas content limits the effectiveness of any one nation's laws. *See* Final Report of the COPA Commission, at 13.

[10] Thornburgh Report, at 365-366. The COPA Commission also analyzed the effectiveness of user-side filtering and blocking technologies. The results indicate that filtering and blocking technologies are more effective for protecting children (and less restrictive of First Amendment values), than the approach taken in the COPA criminal statute. *See* Final Report of the COPA Commission, at 8, 21, 25, 27.

IV. Ineffective, Flawed, and Unconstitutional Legislative Proposals

Congress has before it, and has considered over the past year, a range of proposals intended to protect children online. Most of those proposals, however, would not be effective in furthering that goal, and they raise serious policy or constitutional problems. If enacted, the almost certain result would be lengthy litigations followed by court decisions striking the provisions down (and wasting millions of taxpayer dollars to cover the cost of the litigations). Congress should *not* enact the provisions identified immediately below, but should instead pursue the steps proposed in Part IV.

Mandatory Labeling (S. 49 & H.R. 837): Congress should not impose a mandatory labeling regime on Internet content. Following a number of proposals advanced in 2006, S. 49 and H.R. 837 both include a requirement that a very broad range of completely legal material online must be labeled "sexually explicit." This proposal raises a range of policy and constitutional problems:

- This proposal would be completely ineffective at protecting children. Because hundreds of thousands of adult sites are overseas, the chance that children would be able to access adult sites would be essentially unchanged by this proposal.

- The proposal is unnecessary, because the vast majority of "adult" websites already can be easily blocked by filtering software based on the words and language on the sites. Moreover, the American adult industry (the only adults sites that would be covered) *already* has declared that adult sites should voluntarily label their sites.[11]

- This proposal would apply to – and would stigmatize – a vast array of completely legal content, including content with no nudity or sexual acts. The broad language of the bill would apply to many R rated movies, some PG, PG-13 and TV-PG content, music lyrics, art, and pages of text in online books, magazines and other publications.

- The proposal would undermine the existing MPAA, ESRB, RIAA, and other labeling systems, because consumers would see, for example, content that is rated PG-13 by the MPAA but is declared "sexually explicit" by the federal government.

- The proposal is plainly unconstitutional. Courts have repeatedly struck down measures to attach a "scarlet letter" to legal but disfavored content. Among the many court decisions prohibiting "compelled speech" of the type proposed here is the November 2006 decision of the U.S. Court of Appeals for the Seventh Circuit in *Entertainment Software Association v. Blagojevich*.[12] Moreover, the proposal suffers from the same vagueness and overbreadth problems that the Supreme Court found in the CDA and COPA statutes.

CDT has more fully analyzed the mandatory labeling proposals in letters submitted to the 109th Congress in August 2006, available at http://www.cdt.org/speech/20060803labeling.pdf.

[11] *See* http://www.rtalabel.org/.

[12] Available at http://www.ca7.uscourts.gov/fdocs/docs.fwx?submit=showbr&shofile=06-1012_018.pdf.

Deleting Online Predators Act (S. 49): In 2006, the House approved the Deleting Online Predators Act, which sought to prevent children from using or viewing blogs and social networking sites in schools and libraries. DOPA has again been proposed in S. 49. DOPA raises a range of policy and constitutional problems:

- DOPA would be largely ineffective, in that children who have Internet access at home would simply shift their social networking usage to other times or other avenues (including, for example, the explosion of cell phones that now support access to web sites). Moreover, the vast majority of teens using social networking sites *already* take concrete steps to shield their identity from unknown people.

- DOPA would block minors' access (and burden adults' access in libraries) to a category of speech – mere conversation, including social, political, medical, and an unlimited range of topics – that no court has ever allowed the government to censor or regulate. Just as courts have repeatedly struck down efforts to protect minors by expanding the types of content that can be regulated (to include, for example, violent content), the courts will strike down this effort to create a whole new category of regulated speech.

- Moreover, unlike prior library filtering law ("CIPA") (which regulated *only* content that could lawfully be blocked from minor's access), the vast bulk of the speech blocked by DOPA – teens chatting with their friends, posting photos and linking to their favorite music – is *completely* legal. DOPA would burden a vast quantity of constitutionally protected speech because a very small amount of that speech presents risks to minors. A far better approach would be to educate minors about those risks.

- By completely barring minors from accessing non-educational but wholly legal social conversation sites from libraries or schools, DOPA would prevent some speech from taking place at all, something that the Supreme Court has never permitted in this context.

- DOPA would be a major step backwards in our nation's effort to close the gaping digital divide that exists between affluent families able to bring broadband into the home, and those families whose children can only access the Internet at a school or library. Although affluent teens would be able to connect over the latest and hottest social networking site, those less well off would have no way to interact with their peers online.

- Finally, DOPA is bad policy because it substitutes the one-size-fits-all approach of Congress for the multitude of local-community-determined approaches already being implemented by librarians and school administrators all around the country.

CDT has more fully analyzed the DOPA proposal in report submitted to the 109th Congress in August 2006, available at http://www.cdt.org/speech/20060811dopa.pdf.

Burdens and Liability on Blogs and Social Networking Communities: Congress should not impose new liability on creators of Internet communities. Late last year, S. 4089 (the "Stop the Online Exploitation of Our Children Act") was introduced, proposing to impose significant burdens and liability on blogs and social networking communities. In the new Congress, however, the sponsor of S. 4089 (Senator McCain) modified his proposals to generally avoid burdening blogs and social networking sites (in his S. 431 and S. 519).

Other Members of Congress are considering proposals targeting social networking sites. Proposals that create burdens and liability on service providers run counter to one of the most important provisions in the Telecommunications Act of 1996 – Section 230 (47 U.S.C. § 230) – which protects Internet service and content providers from liability for the content posted by other users on the Internet. Section 230 has been absolutely essential to the protection and promotion of free speech on the Internet, and it has enabled the emergence of the Internet as a place for robust political and social debate. Its protections must be preserved. By imposing burdens and liabilities on blogs and social networking sites, this type of proposal will have a devastating impact on the incentive and ability of small service providers to operate at all.

Issues raised by S. 4089, and burdens on social networking in general, are discussed more fully in a December 2006 posting to CDT's blog, at http://blog.cdt.org/2006/12/11/monitoring-the-would-be-monitors.

Data Retention (H.R. 837): Congress should not impose burdensome data retention requirements. Even though communications service providers and online companies already cooperate extensively with law enforcement investigations, including by preserving user data when requested, an extremely broad and burdensome data retention proposal has been introduced in H.R. 837. Congress should resist data retention proposals, which threaten to place unnecessary burdens on service providers, jeopardize the privacy of innocent users, and chills speech. Proposed data retention obligations in general, and H.R. 837 in particular, raise a host of concerns:

- Data retention laws threaten personal privacy at the very time the public is justifiably concerned about privacy online. One of the best ways to protect privacy is to minimize the amount of data collected in the first place. A data retention law would undermine this important principle, resulting in the collection of large amounts of information that could be misused.

- Mandatory data retention laws could result in large databases of subscribers' personal information, which would be vulnerable to hackers or accidental disclosure. At a time when identity theft is a major concern and security vulnerabilities in the Internet have not been adequately addressed, data retention would aggravate the risk of data breaches and unauthorized use.

- Data retention laws create the danger of mission creep. It is all but certain that the vast databases that ISPs and telecom providers will create will be tapped by law enforcement for other purposes unrelated to child pornography investigations. Service providers themselves might be tempted to use the stored information for a range of currently unanticipated purposes.

- Data retention laws are unnecessary – authority already exists to preserve records. Already, under 18 USC § 2703(f), any governmental entity can require any service provider (telephone company, ISP, cable company, university) to immediately preserve any records in its possession for up to 90 days, renewable indefinitely. If necessary, this "data preservation" authority could be strengthened, and for example could be an automatic requirement whenever an ISP reports possible child pornography to NCMEC (as S. 4089 introduced in December 2006 suggested).

- Data retention laws undermine public trust in the Internet. Subscribers are less likely to use services that compromise the privacy and security of their personal information.

- Data retention laws are burdensome and costly. Data retention laws would require investments in storage equipment and force ISPs to incur large annual operating costs. Currently, Internet access is relatively affordable and therefore available to many. The huge costs associated with data retention would be passed on to consumers, inhibiting efforts to expand Internet access.

- H.R. 837 is particular problematic because it gives unbounded discretion to the Attorney General to set any data retention obligations he deems appropriate. Thus, under H.R. 837, the Attorney General could require all ISPs to retain for 20 years a record of all web surfing, e-mails, and Instant Messages of their customers. The harm to privacy and the financial costs imposed on ISPs (and ultimately on customers) would be enormous under the approach taken by H.R. 837.

- An alternate approach taken by S. 519 and H.R. 876, while still problematic in some respects, offers more cautious and appropriate approach to data preservation. Those proposals would require ISPs to preserve for 180 days any information (pertaining to possible child pornography) submitted by the ISPs to the National Center for Missing and Exploited Children. These proposals, unfortunately, give dangerous powers to the Department of Justice to expand the preservation requirement without any review or input from Congress.

CDT has more fully analyzed the issues raised by data retention proposals in a June 2006 memorandum, available at http://www.cdt.org/privacy/20060602retention.pdf.

Government blacklists of web sites (S. 519 and H.R. 876): There have been a number of proposals discussed to create a blacklist of websites (hosting, for example, child pornography) and require ISPs to block access to those sites. The State of Pennsylvania enacted such a law in 2003, but the requirement had enormous harmful collateral consequences, and ultimately was held to be unconstitutional in a lawsuit initiated by CDT. In that case, CDT proved that in an effort to comply with Pennsylvania orders to block access to about 350 child pornography websites, the ISPs subject to the blocking orders ended up blocking access to more than *1.5 million* wholly unrelated and innocent web sites. The federal court declared that the law violated the First Amendment, and enjoined its enforcement. For more info and the court decision, see http://www.cdt.org/headlines/174.

Congress has not yet considered such a mandatory blocking system, but S. 519 and H.R. 876 both include a critical first step toward such a blocking system – a Congressionally-created blacklist of "Internet addresses" that are alleged (but not proven) to contain child pornography. There are a number of serious difficulties with the blacklist proposal, the most glaring of which is that the government would place sites on the blacklist without any judicial review or oversight whatsoever. Although the blacklist approach may be superficially appealing, it raises very significant constitutional concerns.

V. Effective and Constitutional Legislative Proposals (including H.R. 1008)

Although the proposals discussed above raise serious policy and constitutional concerns, Congress is certainly not powerless to take effective action to promote child safety. Indeed, the blue-ribbon panel chaired by former Attorney General Thornburgh specifically considered and advanced a wide array of alternative public policy recommendations. The Thornburgh Report concluded, for example, that:

- Concrete governmental efforts to promote Internet media literacy and educational strategies would yield superior results without any significant burden on protected speech. Specifically, the Report suggests government funding for the development of model curricula, support of professional development for teachers, support for outreach programs such as grants to non-profit and community organizations, and the development of Internet educational material, including public service announcements and Internet programming akin to that offered on PBS.[13]

- Government support of parents' voluntary efforts to employ technological solutions would provide an effective alternative to criminal laws. While recognizing that filtering technology is not perfect, the Thornburgh Report concludes that filters (which may be installed directly on a computer by end-users or available as a feature offered by an ISP) can have "significant utility in denying access to content that may be regarded as inappropriate."[14]

CDT believes that the Thornburgh Report provides an effective roadmap to promoting child safety online. Congress should promote education of children, and awareness by parents of parental empowerment tools. CDT urges Congress to fund programs to promote media literacy for both adults and children, which are the most effective way to protect children online. And critically, support for educational programs needs to flow not only to specialized non-profit groups, but also to the schools and libraries that are themselves on the front lines of teaching children how to safely and effectively benefit from the wealth of information available on the

[13] Thornburgh Report, at 384-385.

[14] Thornburgh Report, at 303. The COPA Commission also identified a range of governmental actions that it believed would significantly contribute to the protection of children on the Internet. Significantly, the passage and enforcement of new criminal laws (like the COPA statute) was not included in the Commission's recommendations. Many of the Commission's recommendations are similar to those later made by the National Academy committee. *See* Final Report of the COPA Commission, at 39-46.

Internet. Compared to other countries, our investment in technology and media literacy is inadequate and piecemeal in nature.

H.R. 1008 offers an effective approach to support and promote educational efforts about Internet safety. The proposal would direct the Federal Trade Commission to create an office to coordinate Internet safety initiatives, and would authorize federal grants to schools, libraries and others to promote online safety. The proposal, introduce by Congresswoman Melissa Bean, has 49 co-sponsors.

In addition to the critical focus on education for both parents and children, there are a number of important additional steps that Congress can take to enhance child safety online – including proposals that have been included in bills that have already been introduced in Congress. For example, Congress could increase funding for direct prosecution of child pornography and child predation (as proposed by Section 4 of S. 519 and H.R. 876), and encourage foreign governments to enhance their efforts to combat child pornography and exploitation (as proposed by Section 3 of the same two bills).

* * *

CDT would welcome an opportunity to discuss any of the above proposals, or other proposals intended to protect children online. Please contact CDT Executive Director Leslie Harris or Staff Counsel John Morris at (202) 637-9800.