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

Child Safety and Free Speech Issues in the 110th Congress

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

Updated as of February 6, 2008

I. Summary

During the 110th Congress, members of Congress have introduced an unprecedented number of bills intended to protect children on the Internet. CDT strongly believes that protecting minors online 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 child protection measures and would raise very serious policy and constitutional problems.

Congress has twice asked leading panels of experts to provide guidance on the most effective way to protect children online. In both instances, those experts concluded that the best approach to online child safety is to provide comprehensive education about Internet use and safety, 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 more than half of the sexual content that Congress seeks to regulate is overseas, outside the reach of U.S. criminal law or regulation.

Bills that would impose mandates on or limit access to social networking sites are prime examples of well-intended but misguided legislative proposals that do not advance child safety online. The overwhelming majority of communications over such sites are completely appropriate and proposals to restrict minors' access to such sites from school computers would only exacerbate the digital divide and impose unwarranted burdens on educational institutions and web operators. In contrast, Congress can follow the advise of its expert panels and promote comprehensive education of children about the rules and risks of using the Internet, and of parents and caregivers about the use of filtering and other user empowerment 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 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 10 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 10 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 and thus the proposed legislative responses are not well tailored to the risk. American children under 18 engage in 10 million or more online communications every day, and the vast majority of those communications are perfectly innocuous and completely legal. Moreover, academic research indicates that education of children about online predators is a critical approach to the problem.[1]

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

---

[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.

[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 at http://www.copacommission.org/report/.

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 are ineffective, and (B) education and parental empowerment with filtering and other tools are far more effective than any criminal law.

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

---

[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 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.

[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.

> 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.

IV. Ineffective, Flawed, and Unconstitutional Legislative Proposals

Congress has before it a range of proposals intended to protect children online. Many 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 Section V.

The following specific bills are the leading problematic legislative proposals.

"Kids Act" – Sex Offender E-mail Registry (S. 431 – passed by Senate Judiciary Committee): This bill – sponsored by Sens. Schumer & McCain – would require sex offenders to register their e-mail, instant messaging, and other online addresses. Although the bill stops short of mandating that social networking sites screen their users against a database of addresses, there is little doubt that social networking sites of all types would be under political pressure to do so. For that reason, S. 431 would likely reduce the ability of blogging and social networking sites to offer their services for free, and has a number of other serious problems. The House abandoned the e-mail registry proposal – recognizing the range of problems with that approach – and opted in H.R. 719 for a far more focused and effective strategy to limit the Internet access of dangerous sex offenders (and detailed more fully below in Section V). The problems with S. 431 include:

[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.

- The definition of "commercial social networking website" in S. 431 would sweep in many blogs on the Internet and a growing number of commercial and other sites. Because of this overbroad definition, some free or low cost blogging sites would not be able to bear the significant cost of screening their users against the e-mail registry. Thus, it is likely that this bill will serve to reduce the avenues for free and low cost expression on the Internet - the very thing that has made the Internet such a powerful force in our society.

- The superficially "voluntary" nature of the database would in practice not be voluntary, and would thus impose significant costs on a very broad range of websites, including many sites where child predators are not likely to make contact with minors. Although the bill does not make the screening of sex offender addresses a mandatory obligation, pressure from politicians and the media will force many sites – including free and low cost sites – to screen their users. Again, this will likely lead to a reduction of available sites on the Internet, as well as a trend to move websites overseas where they will be less responsive to American concerns.

- In light of the fluidity of online identities, and the trivial ease of creating new identifiers and online addresses, the screening that the bill anticipates would be ineffective. Any sex offender intent on violating release terms by contacting minors will be able to evade the registry simply by creating a new e-mail address.

- Wholly innocent people will be blocked from access to Internet sites because of the great risk of confusion and misidentification, while sex offenders will be able to evade detection. Because many Internet addresses and identifiers are wholly unverified and cannot be linked to verifiable physical addresses or actual identities, such addresses and identifiers are not unique across the Internet. The use by a sex offender of an Internet identifier "jsmith" is likely to lead to the blocking of access by non-offenders who *also* use "jsmith" to access Internet sites.

At the end of the day, this bill will not actually do much to protect kids from anyone intent on harming them, and it will have a negative impact on the free availability of outlets for lawful speech online. **CDT urges Congress to reject S. 431**, and to adopt the more effective and focused approach taken in H.R. 719 (detailed in Part V below).

"Safe Act" – Government Blacklist & other provisions (H.R. 3791 – passed by the House, S. 519, and S. 1965 with regard to certain sections): H.R. 3791 – sponsored by Reps. Lampson & Chabot – was passed by the House under a "suspension" procedure that is intended for non-controversial bills, even though this bill raises very significant constitutional and other problems. S. 519 (sponsored by Sens. McCain, Schumer & Kyl) and S. 1965 (sponsored by Sen. Stevens, Inouye, and others) contain provisions similar to that in H.R. 3791. Although a few provisions of the bills are appropriate (such as extending immunity to ISPs that report child pornography to the National Center for Missing & Exploited Children, NCMEC), the bill has numerous very problematic provisions, including:

- The bill would require Internet and online service providers to "register" with NCMEC – a wholly unprecedented requirement for a medium that has seen extraordinary growth and innovation *precisely* because providing services on the

Internet does *not* require the type of government registration mandate contained in this bill. The registration mandate would likely apply to thousands of small online application providers, and would very likely chill the innovative contributions from such small providers (or drive them overseas).

- The bill would require Internet and online service providers to disclose to NCMEC an extraordinary amount of personal information – including the contents of e-mail – all without *any* judicial supervision or even prosecutorial involvement. Much of the information required to be disclosed could *not* be disclosed to the government without a court order or formal subpoena. Moreover, because NCMEC is in theory a *private* organization, the information disclosed to NCMEC is not covered by the Privacy Act or the Fourth Amendment, and what NCMEC does with the information cannot be determined through the Freedom of Information Act. Absolutely nothing in this bill would prevent NCMEC from maintaining a database tracking the online activities of American citizens who have not been convicted of or even charged with any crime. One section of **S. 1965 – passed by the Senate Commerce Committee** – would also require extensive data reporting, raising serious concerns.

- In creating the new Section 2258C, this bill would authorize the creation of a federal "blacklist" of images and websites that are alleged to contain child pornography, and then distribute the black list to service providers. Sites would be placed on this blacklist even though no prosecutor, judge, or jury has ever reviewed the images and found them to be child pornography. Although such a program might arguably be constitutional when performed by wholly private entities, this bill would make this "blacklist" a federal program, which would flatly violate the First Amendment under the Supreme Court's decision in *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58 (1963). One section of **S. 1965 – passed by the Senate Commerce Committee** – would also create this government blacklist, raising serious constitutional issues. A similar blacklist law was enacted by Pennsylvania, but was then struck down as unconstitutional in a lawsuit initiated by CDT. For more info and the court decision, see http://www.cdt.org/headlines/174.

- By dramatically increasing the fines for failing to report to NCMEC, and by making a failure a criminal matter, the bill would burden and penalize the Internet industry for a problem that is the responsibility of the Department of Justice (DOJ). To the extent there is a problem with ISPs not reporting to NCMEC, the problem is that DOJ has failed to issue the regulations governing the reporting, as Congress required *in 1999*. Simply put, DOJ has never detailed who reports and how reports should be made. All of the big ISPs and service providers are reporting anyway (using voluntary guidelines developed by a trade association in the absence of the DOJ regulations). There is no evidence that the current $50,000 fine is not enough incentive for providers to report to NCMEC, and increased fines would likely not be necessary if DOJ were to ever issue the needed regulations.

CDT strongly urges the Senate to reject H.R. 3791 (and the companion S. 519).

Expansion of NCMEC Mission (H.R. 2517 – passed by House, and S. 1829 – passed by Senate Judiciary Committee): Both bills – sponsored by Rep. Lampson and others in the House, and Sen. Leahy and others in the Senate – would: (a) dramatically increase the funding of the National Center for Missing & Exploited Children (NCMEC), and (b) expand NCMEC's mission far beyond its appropriate areas of expertise. Although CDT does not object to increased funding for NCMEC, **we oppose the expansion of NCMEC's responsibilities into areas far beyond its expertise.** The problematic expansions of NCMEC's mission are:

- Both H.R. 2517 and S. 1829 would require NCMEC to receive "Cybertips" on "unsolicited obscene material sent to a child." Unlike child porn (which is an essentially objective thing to determine), obscenity is highly subjective according to the local community. What might be "obscene" in Virginia (where NCMEC is located) might not be obscene in Las Vegas. NCMEC has no expertise on obscenity, and could not appropriately try to determine "is this obscenity" in the same way it tries to determine "is this child porn." This subpart would involve NCMEC in prosecutorial decision-making on topics about which it has no expertise.

- H.R. 2517 would require NCMEC to receive "Cybertips" on "misleading domain names" and "misleading words or digital images on the Internet." To the extent these terms are relevant to any criminal law, the terms represent pure legal determinations that NCMEC should not be making. NCMEC is in theory a *private* organization and should not be tasked with making prosecutorial decisions.

In addition, the bills add reporting obligations on NCMEC – which we support – but overlooks more than one-half of NCMEC's work, the child pornography Cybertip line, for which there is almost no public information. We suggest that new requirements be expanded to include reporting about the Cybertip line (about child pornography), to include at least (a) how many reports of alleged child porn are received from the public each year, (b) how many of those reports are passed on to law enforcement as likely child porn, (c) how many reports of alleged child porn are received from ISPs and other service providers each year, (d) how many of those reports are passed on to law enforcement, and (e) the average speed of the "passing on" of reports to law enforcement.

V-Chip for the Internet (S. 602 – passed by Senate Commerce Committee): S. 602 – sponsored by Sen. Pryor – would require the Federal Communications Commission ("FCC") to initiate a "notice of inquiry" about the creation of a "V-Chip" that could be mandated for all computers, cell phones, and any other device capable of connecting to the Internet. In 1996, Congress mandated that televisions contain a "V-Chip" capable of blocking the display of content according to ratings. The extension of this concept to the Internet raises a number of serious concerns:

- This proposal is unnecessary because there is already a robust, innovative, and competitive market for "user empowerment" or "parental control" tools and software, without any need for Congressional action.[11] Moreover, an FCC or Congressional

[11] The breadth of user empowerment tools is well documented at http://www.getnetwise.org and Adam Thierer, *Parental Controls and Online Child Protection: A Survey of Tools and Methods* (Washington, DC: The Progress & Freedom Foundation), available at http://www.pff.org/parentalcontrols.

mandate of a "V-Chip" for the Internet would likely chill the competitive marketplace (as the television V-Chip discouraged the development of more innovative tools for TV).

- A governmental mandate that general-purpose computers or other Internet-capable devices implement a particular piece of FCC-determined hardware would radically and harmfully change the way computers have developed over the past 20 years. To have the government take a controlling place at the engineering tables of the computer and Internet industries would be a major blow to innovation.

- The bill would invite the FCC to regulate the Internet – something that Congress has wisely avoided to date. Although the FCC administers the television V-Chip mandate, the Commission has almost no experience with the Internet and in the past has shown a significant deafness to concerns about innovation in this new medium.

CDT urges Congress to reject S. 602.

"Fleeting Expletives" (S. 1780 – passed by Senate Commerce Committee, and H.R. 3559): This bill – sponsored by Sen. Rockefeller and others – would declare that the Federal Communications Commission can prohibit the utterance on broadcast television of a single "fleeting expletive." This bill would make more stark the unconstitutionality of the FCC's approach to broadcast regulation, when individual words are banned wholly apart from their context in a movie, documentary, or show. CDT's concerns about S. 1780 are extensively detailed in a CDT blog posting at http://blog.cdt.org/2007/07/17/bill-could-hasten-demise-of-fcc-indecency-regulation/.

A number of other bills also include very problematic provisions:

Mandatory Labeling (S. 1086 & H.R. 837): Congress should not impose a mandatory labeling regime on Internet content. Following a number of proposals advanced in 2006, S. 1086 (sponsored by Sens. Baucus & Pryor) & H.R. 837 (sponsored by Rep. Smith and others) would require that a very broad range of completely legal material online must be labeled "sexually explicit." This requirement would raise 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.[12]

- 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

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

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*.[13] Moreover, the proposal suffers from the same vagueness and overbreadth problems that the Supreme Court found in the CDA and COPA statutes.

- S. 1086 is particularly problematic because under it Congress would mandate that ICANN (the "Internet Corporation for Assigned Names and Numbers") take certain actions to implement U.S. policy. ICANN, however, should remain independent of the U.S. government. Proposals such as this greatly aggravate the demands by other countries to be able to impose their own policy rules on the Internet. This proposal would significantly undermine the policies of the United States with reference to ICANN.

CDT has more fully analyzed mandatory labeling proposals in letters submitted to the 109th Congress in August 2006, available at http://www.cdt.org/speech/20060803labeling.pdf. **CDT urges Congress to reject S. 1086 and H.R. 837.**

Deleting Online Predators Act (H.R. 1120): The Deleting Online Predators Act, H.R. 1120 (sponsored by Rep. Kirk and others), would prevent children from using or viewing blogs and social networking sites in schools and libraries. 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.

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

- 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 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. **CDT urges Congress to reject H.R. 1120.**

Burdens and Liability on Blogs and Social Networking Communities: More generally, beyond S.431, H.R. 719, and H.R. 1120 discussed above, Congress should not impose new liability or burdens on creators of Internet communities. 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 regulation of social networks, 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 (sponsored by Rep. Smith and others). Congress should resist data retention proposals, which threaten to place unnecessary burdens on service providers, jeopardize the

privacy of innocent users, and chill 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 U.S.C. § 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.

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. **CDT urges Congress to reject H.R. 837.**

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.[14]

- 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."[15]

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

Effective child safety education proposals include:

---

[14] Thornburgh Report, at 384-385.

[15] 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.

SAFER-NET Act (H.R. 3461 – passed by the House): This bill (sponsored by Rep. Bean and others) would require the Federal Trade Commission to create a new office to coordinate online safety efforts, and to create a nationwide campaign to promote online safety. This approach would help to organize and focus federal efforts on online safety. **CDT urges passage of H.R. 3461.**

Internet Safety Education Act (S. 2344 – passed by the Senate Judiciary Committee): This bill (sponsored by Sen. Menéndez) would authorize $10 million of grants each year for five years to support Internet safety education for both children and parents. S. 2344 is similar to H.R. 4134, which was passed by the House, except that the House version directs that half of the money must be awarded to one particular Internet safety organization. S. 2344 is precisely the type of child safety bill that Congress should be passing. As detailed in Section III above, 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 voluntary use of filtering and other technology tools to empower parents to decide what content their children should access. **CDT urges passage of S. 2344.**

Protecting Children in the 21st Century Act (S. 1965 – passed by Senate Commerce Committee): Section 106 of S. 1965 (sponsored by Sens. Stevens, Inouye and others) would encourage Internet safety education in schools that receive federal funds. This is a very positive provision that CDT supports. Unfortunately, the bill also contains very problematic provisions as detailed above in the discussion of the "Safe Act" (H.R. 3791 – passed by the House, and S. 519).

Other effective and constitutional child safety proposals include:

Sex Offender Internet Usage Limits (H.R. 719 – passed by the House): The initial text of H.R. 719 was the same as the highly problematic S. 431 discussed above (proposing an e-mail registry for sex offenders). After consideration of the problems raised by that proposal, the House opted for a much different – and much more focused and effective – strategy. The revised bill (sponsored by Rep. Pomeroy and others) was passed by the House on November 14, 2007. The bill would (a) authorize additional funds to increase supervision of sex offenders who might pose risks for minors online, (b) allows the imposition of specific Internet access limitations (in probation/release terms) on sex offenders who pose risks online, and (c) makes other statutory changes to facilitate the monitoring of sex offenders. **CDT supports these provisions in H.R. 719.**

PROTECT Our Children Act (H.R. 3845 – passed by House, and similar provisions in S. 1738): Both H.R. 3845 (sponsored by Rep. Wasserman Schultz and others) and S. 1738 (sponsored by Sens. Biden & Boxer) would improve law enforcement's efforts against child exploitation, and provide more resources for programs aimed at protecting children. **CDT urges passage of H.R. 3845.**

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 one section in S. 519), and encourage foreign governments to enhance their efforts to combat child pornography and exploitation (as proposed by another of the same bill).

* * *

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