
POLICY POST

June 6, 1995
Number 16

CENTER FOR DEMOCRACY AND TECHNOLOGY

A briefing on public policy issues affecting civil liberties online
---
CDT POLICY POST Number 16 June 6, 1995

CONTENTS: (1) Sens. Dole & Grassley to introduce sweeping anti-indecency Internet censorship bill
(2) Sen. Lott To offer amendment to strike 'Defenses' section of Exon CDA
(3) Legislative Update -- Status of Exon CDA
(4) Text of the Grassley/Dole proposal
(5) Petition Update -- 20,000 + signaures in the first two weeks
(6) About CDT/Contacting Us

---

(1) SENS DOLE (R-KS) & GRASSLEY (R-IA) TO INTRODUCE SWEEPING ANTI-INDECENCY INTERNET CENSORSHIP BILL

OVERVIEW

Senator Bob Dole (R-KS) is expected to up the ante on Internet censorship tomorrow by co-sponsoring legislation with Senator Charles Grassley (R-IA). The proposal to be offered by the Senate Majority leader and Republican Presidental candidate is more sweeping than the Exon Communicatons Decency Act, and comes on the heals of his recent attack on "sex and violence" in the entertainment industry.

The Dole/Grassley proposal represents an even greater threat to the First Amendment and the free flow of information in cyberspace than the Exon Communications Decency Act, now pending before the Senate (a vote on the CDA is expected as early as tomorrow, 6/7/95). Senator Dole is expected to announce his support for the bill at a 6/7 lunch hosted by the anti-pornography group Enough Is Enough. The text of the proposal is attached below.

Senator Grassley's staff has informed CDT that he bill will be

introduced as a free standing bill and NOT AS AN AMENDMENT TO THE PENDING SENATE TELECOMMUNICATIONS REFORM BILL (S. 652). CDT hopes that the Dole/Grassley bill will not be fast-tracked (as was the Exon legislation), and that hearings will be held on the proposal.

The introduction of Dole/Grassley creates an even greater need for support of Senator Leahy's alternative (S. 714). If the Senate rejects Senator Leahy's alternative, it will pass either the Exon bill or the even more draconian Dole/Grassley proposal, and the net as we know it will never be the same again. To find out what you can do to help, contact the Voters Telecommunications Watch (VTW) by sending a message to vtw@vtw.org with a subject "send alert". Please also sign the petition (URL and instructions at the end of this post)

SUMMARY OF DOLE/GRASSLEY PROPOSAL

The Dole/Grassley bill would create new penalties in Title 18 for all operators of electronic communications services who knowingly transmit indecent material to anyone under 18 years of age. The bill would also create criminal liability for system operators who willfully permit minors to use an electronic communications service in order to obtain indecent material from another service.

The Dole/Grassley bill would impose criminal liability on online service providers, electronic bulletin board operators, as well as any other entity that uses computer storage to deliver information to users, including video dialtone services, cable television video on demand services, etc. The degree of knowledge required to impose liability is unclear, but it appears that an entity could be said to have the requisite knowledge if it is merely informed by a third party that some material on its system is indecent. The text of the proposal is available below.

---

(2) SEN. LOTT (R-MISS) TO OFFER AMENDMENT TO STRIKE 'DEFENSES' SECTION OF EXON CDA.

Senator Lott is preparing to offer an amendment to strike the service provider defenses from the Exon language already approved by the Senate Commerce committee.

Analysis: Holding service providers such as America Online and Internet access providers liable for the content on their system over which they have no control will stifle the free flow of information in cyberspace and create major business risk for the private companies that are building the National Information Infrastructure. Furthermore, placing criminal liability on service providers poses a serious risk to the privacy of individual users by forcing service providers to monitor communications in order to limit their own liability.

Status: Lott plans to offer this amendment when the on the Senate floor when the telecommunications bill is being considered.

---

(3) LEGISLATIVE UPDATE -- STATUS OF EXON CDA

With the Senate telecommunications reform bill poised to go to the floor this week, proposals to censor the Internet are proliferating beyond just the Exon language. The most sweeping and threatening proposals come from the Senate leadership and other Republicans. The provisions of the Exon proposal that are already in the telecommunications bill contain restrictions on indecent communications which would apply to all parts of the Internet, commercial online services, and all other interactive media including interactive television, etc. We believe these provisions to be unconstitutional and continue to oppose them. CDT continues to work with members of the Interactive Working Group in urging support for the Leahy study bill as an alternative.

The Exon proposal now part of the Senate telecommunications bill still poses serious risks to free speech online. The Exon proposal contains restrictions on "indecent" communications, which could ban all sexually-explicit communications on the Internet, along with all uses of the "seven dirty words."

Analysis: CDT continues to argue that the indecency restrictions in the Exon bill are unconstitutional under the First Amendment.

Status: Senator Leahy plans to offer an amendment to strike the Exon provisions and replace them with his study bill (S.714) as an alternative.

CDT continues to work with members of the Interactive Working Group in urging support for the Leahy study as an alternative to the Exon bill, which we still believe to be unconstitutional.

For more information, see CDT's Communications Decency Act Archives:

http://www.cdt.org
ftp://ftp.cdt.org/pub/cdt/policy/freespeech/00-INDEX.FREESPEECH

---

(4) TEXT OF THE DOLE/GRASSLEY PROPOSAL

104th Congress: First Session.

IN THE SENATE OF THE UNITED STATES

Mr. Grassley introduced the following bill, which was read twice and referred to the Committee on

_____

A BILL

To amend section 1464 of title 18, United States Code, to punish transmission by computer of indecent material to minors.

Be it enacted by the Senate and House of Representatives of the United States of American in Congress assembled,

SECTION 1: TRANSMISSION BY COMPUTER OF INDECENT MATERIAL TO MINORS.

(a) OFFENSES. -- Section 1464 of title 18, United States Code, is amended --

(1) in the heading by striking "Broadcasing obscene language" and inserting "Utterance of indecent or profane language by radio communication; transmission to minor of indecent material from remote computer facility, electronic communications service, or electronic bulletin board service";

(2) by striking "Whoever" and inserting "(a) UTTERANCE OF INDECENT OR PROFANE LANGUAGE BY RADIO COMMUNICATION. -- A person who"; and

(3) by adding at the end the following:

"(b) TRANSMISSION TO MINOR OF INDECENT MATERIAL FROM REMOTE COMPUTER FACILITY, ELECTRONIC COMMUNICATIONS SERVICE, OR ELECTRONIC BULLETIN BOARD SERVICE PROVIDER.--

"(1) DEFINITIONS -- As used in this subsection --

"(A) the term 'remote computer facility' means a facility that --

"(i) provides to the public computer storage or processing services by means of an electronic commu nications system; and

"(ii) permits a computer user to transfer electronic or digital material from the facility to another computer;

"(B) the term 'electroni communications service' means any wire, radio, electromagnetic, photo optical, or photo-electronic system for the transmission of electronic communications, and any computer facility or related electronic equipment for the electronic storage of such communications, that permits a computer user to transfer electronic or digital material from the service to another computer; and,

"(C) the term 'electronic bulletin board service' means a computer system, regardless of whether operated for commercial purposes, that exists primarily to provide remote or on-site users with digital images or that exists primarily to permit remote or on-site users to participatein or create on-line discussion groups or conferences.

"(2) TRANSMISSION BY REMOTE COMPUTER FACILITY OPERATOR, ELECTRONIC COMMUNICATIONS SERVICE PROVIDER, OR ELECTRONIC BULLETIN BOARD SERVICE PROVIDER. -- A remote

computer facility operator, electronic commu-
nications service provider, electronic bulletin board service provider
who, with knowledge of the character of the material, knowingly or
recklessly --

"(A) transmits from the remote computer facility, electronic
communications service, or electronic bulletin board service provider a
communication that contains indecent material to a person under 18 years
of age; or

"(B) causes or allows to be transmitted from the remote computer
facility, electronic communications service, or electronic bulletin
board a communication that contains indecent material to a person under
18 years of age,

shall be fined in accordance with this title, imprisoned not more than
5 years, or both.

"(3) PERMITTING ACCESS BY MINOR. -- Any person who
willfully permits a person under 18 years of age to use a remote com-
puting service, electronic communications service, or electronic
bulletin board service to obtain indecent material from another remote
computing service, electronic communications service, or electronic
board service, shall be fined not more than $10,000, imprisoned not
more than 2 years, or both.

"(4) NONAPPLICABILITY TO PARENT OR LEGAL
GUARDIAN. -- This subsection shall not apply to a parent or legal
guardian who provides indecent material to the child of such parent
or legal guardian."

---

(5) PETITION UPDATE -- 20,000 SIGNATUES IN TWO WEEKS.

In the first two weeks of the petition effort, we have gathered over
20,000 signatures in support of Senator Leahy's alternative to the Exon
Communications Decency Act.

If you have not yet signed the petition, please visit the petition page

http://www.cdt.org/petition.html

If you do not have access to the Web, send a message to vtw@vtw.org with
a suject 'send petition' for instructions on how to sing by email.

The petition may be Delivered to Senator Leahy sometime this week, but
it will continue to be up to gather signatures until the House of
Representatives votes later this summer. Updates and a final singature
tally will be posted shortly.

---

(6) ABOUT THE CENTER FOR DEMOCRACY AND TECHNOLOGY/CONTACTING US

The Center for Democracy and Technology is a non-profit public interest organization. The Center's mission is to develop and advocate public policies that advance constitutional civil liberties and democratic values in new computer and communications technologies.

Contacting us:

To subscribe to CDT's news distribution list (to receive future Policy Posts directly), send email to <cdt-lists@cdt.org> with a subject of 'subscribe policy posts'.

NOTE TO THOSE WHO HAVE ALREADY REQUESTED TO BE ADDED TO CDT's DISTRIBUTION LIST: We are still working to build our listserv -- you will beging receiving Policy Posts on this list very soon. We appreciate your patience!

General information on CDT can be obtained by sending mail to <info@cdt.org>

CDT has set up the following auto-reply aliases to keep you informed on the Communications Decency Act issue.

For information on the bill, including CDT's analysis and the text of Senator Leahy's alternative proposal and information on what you can do to help -- cda-info@cdt.org

For the current status of the bill, including scheduled House and Senate action (updated as events warrant) -- cda-stat@cdt.org

World-Wide-Web:

http://www.cdt.org/

ftp:

ftp://ftp.cdt.org/pub/cdt/

gopher:

CDT's gopher site is still under construction and should be operational soon.

snail mail:

Center For Democracy and Technology
1001 G Street, NW Suite 700 East
Washington, DC 20001

voice: +1.202.637.9800
fax: +1.202.637.9800
###

POLICY POST

June 14, 1995
Number 17

CENTER FOR DEMOCRACY AND TECHNOLOGY

A briefing on public policy issues affecting civil liberties online
---
CDT POLICY POST Number 17 June 14, 1995

CONTENTS: (1) Senator Harkin Amendment Seeks to Expand Law Enforcement Access to Telephone Subscriber Information
(2) Text of CDT/ACLU Letter to Harkin
(3) CDA Update -- VOTE EXPECTED TODAY!
(4) About CDT/Contacting Us

---

(1) Senator Harkin Amendment Would Expand Law Enforcement Access and Gut Privacy Protections For Telephone Subscriber Information

Yesterday, CDT became aware that Senator Tom Harkin is planning to introduce an amendment to the Telecommunications Competition and Deregulation Act of 1995 (S. 652) currently being debated on the Senate floor. Harkin's proposed amendment would eliminate the Fourth Amendment protections currently in 18 USC Sec. 2703 and would give law enforcement access to subscriber and customer information on telemarketers from an electronic communications service provider with the presentation of a mere written notice.

Harkin's proposal threatens to undermine severely the privacy protections on personal information held by communications providers. If Harkin's amendment passes, it would open the door to the future unraveling of this section which now requires the government to present a court order, warrant, or subpoena in order to obtain subscriber information.

The Senate is expected to vote on the Harkin Amendment as early as today. CDT urges you to contact Senator Harkin to express your concern about his prposal.

To Contact Senator Harkin:

Phone: +1.202.224.7303
by email: tom_harkin@harkin.senate.gov

---

(2) Text of CDT/ACLU Letter to Sen. Harkin

June 13, 1995

The Honorable Tom Harkin
United States Senator
SH-531 Hart Senate Office Building
Washington, DC 20510-1502

Dear Senator Harkin:

We are writing to register our strong opposition to your proposed amendment to the Telecommunications Competition and Deregulation Act of 1995 (S. 652) which would amend 18 U.S.C. Sec. 2703(c)(1)(B), which provides privacy safeguards for telecommunication subscriber information by controlling government access. Under your proposal, law enforcement could gain access from a telecommunications service provider to subscriber information upon mere submission of a "formal written request" where the subscriber is a telemarketer. This proposal represents a severe departure from the strict Fourth Amendment framework that governs law enforcement access to personal communications and information under Title 18. Under ¤2703, law enforcement officers must first present a warrant, court order, or administrative subpoena to an electronic communications service provider prior to disclosures of information about its subscribers. This section acknowledges the important privacy interest people have in the personal information held by electronic communications service providers. Your proposal would require information to be provided with fewer privacy protections than currently exist even in the case of a foreign counter-intelligence investigation.

The Fourth Amendment privacy protections embodied in Title 18 are the product of a long and thorough debate in which the concerns of law enforcement and the rights of citizens were aired and carefully balanced. Your proposed amendment would unravel this delicate balance without the deliberative process necessary to carve out any exception to standard Fourth Amendment protections.

The proposed amendment suggests that the available mechanisms offered in Title 18 are inadequate to address the problem of telemarketing fraud. However, there has been no opportunity to create a record of the problem or the necessity of amending existing law. We oppose weakening of court order requirements of Title 18. We do not believe that this instance justifies opening the door on eliminating the strong Fourth Amendment privacy protections -- rendering other future "exceptions" to these privacy protections a virtual certainty.

We agree, telemarketing fraud is a serious problem and we are available to meet with you to discuss means of addressing it. We encourage you to seek hearings on this issue so that a full record is developed and appropriate remedies, tailored to the problem, are

crafted. However, we must adamantly oppose your proposed amendment to the Telecommunications Competition and Deregulation Act. We look forward to working with you.

Center for Democracy and Technology

American Civil Liberties Union
Washington National Office

--
For more information contact:

The Center For Democracy and Technology
Janlori Goldman or Deirdre Mulligan (202) 637-9800

ACLU
Don Haines (202) 675-2322

---

(3) CDA Update -- SENATE VOTE EXPECTED TODAY OR TOMORROW

The Senate vote on the Communications Decency Act will occurr either today (6/14) or tomorrow (6/15). Senator Exon has joined forces with Senator Coats (R-IA), and has introduced a revised Exon/Coats Communications Decency Act amendment. The text of this proposal was not available for posting at the time of this writing, but will be made available as soon as we have it.

The Exon/Coats proposal is reportedly similar to the earlier Exon proposals, and would severely restrict the free speech and privacy rights of all Internet users. In addition, the Exon/Coats proposal adds a provision to ban the dissemination of indecency on all cable channels. This would ban the showing of popular programs like NYPD Blue, Melrose Place, educational programing dealing with reproduction, and other programming, and is a clear violation of longstanding Constitutional precedent.

Senator Leahy plans to offer his alternative (S. 714) during the debate today, but the outcome at this point is uncertain. Your help is needed now. For instructions on what you can do (including a list of Senate Contacts), send a message to vtw@vtw.org with a subject "send alert" (w/o the quotes).

CDT is closely following developments on this issue, and will post further information as soon as it becomes available.

---

(4) ABOUT THE CENTER FOR DEMOCRACY AND TECHNOLOGY/CONTACTING US

The Center for Democracy and Technology is a non-profit public interest organization. The Center's mission is to develop and advocate public policies that advance constitutional civil liberties and democratic values in new computer and communications technologies.

Contacting us:

To subscribe to CDT's news distribution list (to receive future Policy Posts directly), send email to <cdt-lists@cdt.org> with a subject of 'subscribe policy posts'.

NOTE TO THOSE WHO HAVE ALREADY REQUESTED TO BE ADDED TO CDT's DISTRIBUTION LIST: We are still working to build our listserv -- you will begin receiving Policy Posts on this list very soon. We appreciate your patience!

General information on CDT can be obtained by sending mail to <info@cdt.org>

CDT has set up the following auto-reply aliases to keep you informed on the Communications Decency Act issue.

For information on the bill, including CDT's analysis and the text of Senator Leahy's alternative proposal and information on what you can do to help -- cda-info@cdt.org

For the current status of the bill, including scheduled House and Senate action (updated as events warrant) -- cda-stat@cdt.org

World-Wide-Web:

http://www.cdt.org/

ftp:

ftp://ftp.cdt.org/pub/cdt/

gopher:

CDT's gopher site is still under construction and should be operational soon.

snail mail:

Center For Democracy and Technology
1001 G Street, NW Suite 700 East
Washington, DC 20001
voice: +1.202.637.9800
fax: +1.202.637.9800
###

POLICY POST

June 14, 1995
Number 18

CENTER FOR DEMOCRACY AND TECHNOLOGY

A briefing on public policy issues affecting civil liberties online
---
CDT POLICY POST Number 18 June 14, 1995

CONTENTS: (1) Senate Passes CDA -- Battle Moves to House
(2) About CDT/Contacting Us

---

(1) Senate Passes Exon/Coats -- Battle Moves to House

The First Amendment was thrown out of cyberspace by the United States Senate today by a vote of 84 to 16 on passage of the Exon/Coats Communications Decency Act.

CDT remains adamantly opposed to this legislation, and we will continue to fight it as the bill moves to the House of Representatives. A House vote is expected in mid July.

In his effort to defeat the Exon amendment, Senator Leahy cited the over 35,000 signatures on the Internet petition, as well as the serious First Amendment and privacy concerns raised by the Exon proposal. Senator Feingold (D-WI) also spoke in opposition to the Exon amendment, and asked that the Senate consider the unique features of interactive media. Unfortunately, these efforts to protect the Internet from unnecessary and repressive censorship were not successful.

A full analysis of the Senate passed bill, as well as a description of the events that occurred today on the Senate floor will be posted in the next few days.

---

(2) About The Center For Democracy And Technology/Contacting Us

The Center for Democracy and Technology is a non-profit public interest organization. The Center's mission is to develop and advocate public

policies that advance constitutional civil liberties and democratic values in new computer and communications technologies.

Contacting us:

To subscribe to CDT's news distribution list (to receive future Policy Posts directly), send email to <cdt-lists@cdt.org> with a subject of 'subscribe policy posts'.

NOTE TO THOSE WHO HAVE ALREADY REQUESTED TO BE ADDED TO CDT's DISTRIBUTION LIST: We are still working to build our listserv -- you will begin receiving Policy Posts on this list very soon. We appreciate your patience!

General information on CDT can be obtained by sending mail to <info@cdt.org>

CDT has set up the following auto-reply aliases to keep you informed on the Communications Decency Act issue.

For information on the bill, including CDT's analysis and the text of Senator Leahy's alternative proposal and information on what you can do to help -- cda-info@cdt.org

For the current status of the bill, including scheduled House and Senate action (updated as events warrant) -- cda-stat@cdt.org

World-Wide-Web:

http://www.cdt.org/

ftp:

ftp://ftp.cdt.org/pub/cdt/

gopher:

CDT's gopher site is still under construction and should be operational soon.

snail mail:

Center For Democracy and Technology
1001 G Street, NW Suite 700 East
Washington, DC 20001
voice: +1.202.637.9800
fax: +1.202.637.9800
###

POLICY POST

June 20, 1995
Number 19

CENTER FOR DEMOCRACY AND TECHNOLOGY

A briefing on public policy issues affecting civil liberties online
---
CDT POLICY POST Number 19 June 20, 1995

CONTENTS: (1) CDT Analysis of Senate Passed Exon/Coats Communications Decency Act
(2) Text of the Statute With Proposed Amendment
(3) About CDT/Contacting Us

---

(1) CDT Analysis of Senate Passed Exon/Coats Communications Decency Act

The United States Senate last week approved sweeping Internet censorship legislation which dramatically restricts the free flow of information in interactive media, and fails to even provide effective protection for children from access to inappropriate information. The Center for Democracy and Technology strongly opposes the Exon/Coats Communications Decency Act for the following reasons:

UNCONSTITUTIONAL BAN ON "INDECENT" MATERIAL IN MOST PARTS OF THE INTERNET: The Act imposes criminal penalties of $100,000 fines or up to two years in prison on anyone who "knowingly ... makes or makes available any indecent communications ... to any person under 18 years of age." This restriction on indecency (a legal term which includes the "seven dirty words" as well as any sexually-explicit material) amounts to a total ban on all "indecent" information in public areas of the Internet, since all users of the Internet know that public areas are accessible to minors. The United States Supreme Court has held over and over again that indecent material is protected by the First Amendment and may only be regulated with narrowly tailored means that leave adults free to communicate. Senator Exon's bill has failed to identify Constitutionally-appropriate means of regulation. As Senator Leahy pointed out during the Senate debate, the Exon bill would force everyone on the Internet to behave as if there were in "Sunday school."

SECOND-CLASS FREE SPEECH RIGHTS FOR ALL INTERACTIVE MEDIA: The Exon/Coats amendment diminishes the First Amendment rights of those who use interactive media as opposed to those who communicate through print. The

indecency ban in Exon/Coats creates the paradoxical result that speech which would be fully-protected in books, magazines, newspapers, or other print-based publications, would be subject to criminal sanction if made available over the Internet. In other words, what is legal in all of the nation's bookstores would become illegal in cyberspace.

CRIMINALIZATION OF "ANNOYING" MESSAGES: Annoying someone using harsh (but not obscene) language over interactive media would become a crime, also punishable by $100,000 fines and two year jail terms. Federal and many state laws already criminalize harassment, no matter what the medium, but prohibiting mere annoyance is clearly unconstitutional and a wasteful abuse of federal power.

FEDERAL COMMUNICATIONS COMMISSION JURISDICTION OVER CONTENT AND TECHNICAL STANDARDS ON THE INTERNET: Enforcement of the Exon/Coats bill will require extensive an ongoing FCC proceedings to determine what exactly constitutes "indecency" in various interactive media, and how the "safe harbor" defenses in the bill will function. Such regulation will mean that the FCC intrude on the development of all current and future Internet standards for services such as the World Wide Web, electronic mail, and Usenet newsgroups. CDT believes that such an FCC role will lead to unnecessary confusion and delay in the growth of the Internet, as well as cast a continual chill over all speech on the Internet and other interactive media.

PROVISIONS DESIGNED TO PROTECT ONLINE SERVICE PROVIDERS FROM LIABILITY ARE INEFFECTIVE: The "defenses" to prosecution that are intended to protect online services and Internet access providers from liability will create significant risk of criminal liability for all services that provide access to the Internet. Though Senator Exon may originally promised to exempt these providers from liability, his last-minute compromise with Senator Coats, and failure to understand the basic operation of Internet services, left all Internet access providers at risk of criminal liability for providing access to Usenet newsgroups and other public information services.

"GOOD FAITH DEFENSE" FOR SERVICE PROVIDERS MAY ENCOURAGE VIOLATIONS OF USER PRIVACY: Section (f)(4) of Act insulates online service providers from any contractual liability that may arise from their efforts to restrict minors' access to indecent material. Because of the vaguaries of the Electronic Communications Privacy Act regarding service provider access to subscriber email for "system maintenance purposes," this provision may imunize online service providers who read private messages of their users in circumstances where the provider is acting within the bounds of the Exon/Coats bill.

UNDUE BURDEN ON INDIVIDUAL USERS, CONTENT PROVIDERS, AND SMALL SYSTEM OPERATORS: Although Senator Exon claims that his bill is only an extension of the dial-a-porn law, it is actually far broader. The dial-a-porn law applied only to commercial providers of 900 number services, not every telephone customer in the country. Given the fact that every Internet user is both publisher and a receiver of information, Exon's new law, if enacted, would create new regulations on the speech of all those who use interactive media.

In simple terms, the Communications Decency Act would enshrine in statute a sharp distinction between the print medium and new interactive media. For example, though an individual is allowed to go into a bookstore and buy a sexually-explicit magazine or a "lewd" work of art, one would not be able to access the identical information over the Internet. Both the interactive media and the print media are arenas in which individuals and organizations exercise core First Amendment free speech rights. Before Congress elects to diminish the First Amendment protections available in this new medium, we believe that careful, public consideration is required.

A. UNCONSTITUTIONAL RESTRICTIONS ON INDECENT SPEECH ONLINE: BANNING THE"SEVEN DIRTY WORDS" ON THE NET.

If this new proposal became law, the level of discourse on the Internet as a whole would have to be reduced to that which is considered appropriate for children. A newly added section (e) effectively makes it illegal to use any of the "seven dirty word" in public forums on the Internet. This new subsection makes in a crime to "knowingly" make and transmit an indecent message to anyone under 18 years old. This provision covers both private messages between two individuals and public postings to newsgroups that may well reach hundreds of thousands of people around the world. Though the drafters may want to limit this crime to situations where material is provided directly to minors, that is simply impossible on the net. Anyone who participates in public discussion groups knows that there may well be kids reading the group as well. Thus, they would be violating the law simply by posting a hotly-worded message.

Examples of Prohibited items under the new subsection (e)

Rap music lyrics (both the text and the sound files)
Lady Chatterly's Lover
Public declaration that you're "pissed off" or that someone is a "shit."
Calvin Klein advertisements (the ones with naked bodies)

The constitutional flaw in this section lies in the critical distinction between "obscenity," that which is truly hard-core pornography, and "indecency," sexually-explicit material which may be offensive to some or may be considered by some to be inappropriate for children, but which is protected by the First Amendment. Under the First Amendment, Congress has broad power to ban obscenity, but can only regulate indecency in very narrow circumstances, such as in the broadcast media where there is a captive audience. Pacifica Foundation v. FCC (1978) . Even in these narrow circumstances, such regulation may be the "least intrusive means" for accomplishing the government's goal of protecting children. Sable Communications v. FCC. Given the existence of software and hardware that enable parents to block children's access to indecent material the regulation here does not constitute the "least restrictive means" requirement set out by the Supreme Court.

CDT believes that the Act as drafted would not survive a First Amendment

challenge under the law of Sable because the Senate has altogether failed to investigate less restrictive alternatives to meeting its goal of protecting children. The Senate has held no hearings and made no legislative findings which support its decision. During the debate on the Senate floor, both Senator Leahy and Senator Feingold offered evidence that there are less restrictive alternatives available. Neither Senator Exon, Senator Coats, no any other Senator rebutted or responded to these assertions. In light of the overwhelming evidence that users and parents can exercise control over what they and their children receive over the Internet, a court reviewing the constitutionality of the bill, would, we believe, be forced to return the matter to Congress for further consideration.

Furthermore, the government may not regulation indecent material in a way that would deny adults access to such material. Butler v. Michigan (1957). This is precisely the result that is produced by this new statutory proposal. Such as result would be both unwise and unconstitutional. The highly restrictive treatment proposed here for interactive media creates a situation in the future whereby material that is legally available to people of all ages in bookshops and libraries will be banned from the Internet. During the Senate debate, Senator Feingold also pointed out that there are many kinds valuable information on the Internet that might be considered indecent under FCC definitions, such as AIDS education information, various works of art, etc.

B. INTRUSION OF THE FEDERAL COMMUNICATIONS COMMISSION ON CONTENT AND STANDARDS IN INTERACTIVE MEDIA

There are "defenses to prosecution" under this statute which are designed to limit the liability of service providers and, possibly, users and content creators. (See subsection (f)) To avoid being prosecuted under this statute an entity can take "good faith steps" to restrict access to the possibly infringing communications and then hope that if charged with violating the Act, that the court believes you took sufficient steps. A more prudent person, or a corporation with money and reputation at risk, would more likely wait to see what the FCC says are sufficient steps to restrict access and follow those regulations. Until the FCC acts, the defenses applicable to the dial-a-porn law are available, but it is not clear how they would apply to interactive media.

If this provision were to become law, an FCC rulemaking will be required to decide two issues:

1) what is indecent in interactive media?

This could include the "seven dirty words", frontal nudity, sound files with heavy breathing, or many other examples. However, granting the Federal Communications Commission the authority to answer to this question would bring the Internet under a similar content regime as broadcast television and radio.

2) what steps must be taken to restrict access to indecent material?

The FCC will also have to decide what techniques must be used to restrict access sufficiently to enable users and providers to avoid criminal liability. FCC intrusion in the rapidly evolving interactive media market promises to delay the development of new technologies, squelch the entrepreneurial spirit which has helped the Internet to grow, and chill the speech of all users and content creators. The FCC took 8 years to get blocking rules settled just for 900# services, and that was one relatively simple technology. Giving the FCC authority to set child-access standards for every piece of the Net, and all new Net services that develop is a disaster for the medium and will have a sweeping chilling effect on both the technology and free expression online.

As Senator Leahy noted during debate on the bill, "the Internet has become the tremendous success it is because it did not have Big Brother, the Federal Government, trying to micromanage what it does and trying to tell users what it could do. If the Government had been in charge of figuring out how to expand the Internet or make it more available and so on, I guarantee it would not be one-tenth the success it is today." (Cong. Rec. 8344)

C. A NEW CRIME OF ONLINE ANNOYANCE

Senator Exon proposes criminal sanctions for anyone who uses "obscene, lewd, lascivious, filthy, or indecent" communications "with intent to annoy, abuse, threaten, or harass another person." Federal and state laws already punish criminal harassment, regardless of the medium used to perpetrate the crime. (See 18 USC 875(c)). CDT believes that additional laws in this area are simply unnecessary. Moreover, the Department has Justice has said that it has adequate prosecutorial powers in this new environment. (See DoJ letter June 14, 1995).

D. LIMITATIONS ON SERVICE PROVIDER LIABILITY ARE WEAK AND THREATEN TO RADICALLY REDUCE THE DECENTRALIZED NATURE OF THE INTERNET

Some provisions of the Exon/Coats bill attempt to limit the liability of service providers where they act only as passive transmitters of content. However, these provisions have been significantly weakened as a result of pressure from anti-pornography groups, and are subject to interpretation which creates great risk for both users and service providers. Anti-pornography groups have been pressing to hold online providers responsible for all of the information accessible to minors on the Internet. The earlier version of the Exon bill excused from criminal liability anyone who had no editorial control over the content of the message. However, the bill passed by the Senate removed the "editorial control" defense. Instead, service providers could limit their liability only if they "ha[ve] no control" over the service, or if they take steps to restrict access for minors. The degree of nature or degree of control which could leave a provider open to liability is, however, not specified. CDT believes that these weakened "defenses"

leave access providers, and thus Internet users, in a state of great uncertainty as to their responsibility under this bill.

One of the major criticisms of the original legislation introduced by Senator Exon in February 1995 was that it placed criminal liability on online service providers and Internet access providers for any content that traveled across their networks. In response to these criticisms, Senator Exon altered his bill to assure that service providers would not be held responsible for content on their network unless they exercised editorial control. However, in the final days before Senate action on the bill, Senator Exon changed the provisions again at the request of Senator Coats. Now, the presumption of liability has been reversed and a service provider would have to show that it has no control over the service which carried indecent content to a particular minor.

THE END OF USENET NEWSGROUPS?

The major uncertainty of the defenses centers on what it means for a service provider to have control over indecent or obscene content. The uncertainty of this defense is revealed in an analysis of an Internet access providers relationship and potential criminal liability for providing access to Internet newsgroups such as Usenet. Most Internet service providers provide access to Usenet, and, generally make choices about which newsgroups they carry. Some carry all newsgroups, others carry only some groups. The architecture of the Internet newsgroup system is such that a particular Internet access provide can chose to exclude the "alt.sex" newsgroups, or not. Does this ability to exercise control mean that the service provider is criminally liable under the statute? Or, does a carrier have to actually exercise control over the content of individual messages? These definitional questions are legal fine points, but create substantial uncertainty over the meaning of the Act and are likely to lead to litigation and instability in the Internet environment. Until these issues are resolved, there will likely be a substantial chilling effect on all speech on such services.

The bill and associated legislative history leave some doubt as to the meaning of control, since it is never explicitly defined. Debate on the Senate floor, which is often used by courts to divine the legislative intent of the drafters where a statute is unclear, gives seemingly contradictory signals on the question of service provider liability for services such as Usenet newsgroups. One the one hand Senator Exon says in the Congressional Record of the debate that an online provider merely providing access, navigational tools and incidental services "is not aware of the contents of the communications and should not be responsible" for violation of the obscenity, indecency or harassment crimes in the Act. (Cong. Rec., S8345). On the other hand, Senator Coats, the co-sponsor of the bill, says that the Act "does not create a defense for someone who has some level of control over the material of the provision of the material." (Cong. Rec. S8345). Senator Exon also says in the course of this "colloquy" with Senator Coats that those "engaging in pornography and indecency should install 'electronic bouncers' at their electronic doors" to keep minors out. (Id.)

CDT believes that defenses to prosecution for online service providers are critical in the context of this legislation, but is concerned that the defenses no longer serve the function for which they were originally designed. As written in the Senate-passed bill, the defenses appear to require Internet service providers to interfere with the content of messages on their networks if they have any ability to do so.

CREATION OF NEW GATEKEEPERS

Forcing online services providers to exercise control as the new Exon/Coats bill seems to require would spell the end of the open, decentralized communications environment which has characterized the Internet until now. As we have argued elsewhere, users and parents have a great degree of control over what they and their children receive in interactive media. Federal policy should encourage the development of this user control potential, rather than return to the centralized control regulatory models which characterized the mass media. As an open, decentralized medium, the Internet promotes the free flow of information and serves as a valuable political and cultural forum. If we rely on user control technology we can protect children without involving federal regulators in the censorship of constitutionally-protected speech.

E. UNFAIR TREATMENT OF INDIVIDUAL USERS, EDUCATIONAL INSTITUTIONS AND OTHER NON-COMMERCIAL SERVICES: PRE-EMPTION AGAINST RESTRICTIVE STATE LAWS ONLY FOR COMMERCIAL SERVICES

If enacted, this proposal would protect commercial service providers from additional censorship by state legislatures, but leave all non-commercial users, including libraries, schools, community groups, and individuals subject to additional regulation and censorship under state law. The proposal pre-empts state statutes that might censor commercial services beyond the scope of federal law, but leaves all other net users and groups exposed to any censorship that states may choose to enact. We find no valid public policy argument which would accord greater protection to commercial speech than is granted to non-commercial users of the net.

CONCLUSION: Failure to take full advantage of user and parental control features inherent in interactive media

Legislating about new interactive media requires a careful understanding of the unique attributes of this new medium. First and foremost, interactive media enable users (including parents) to exercise choice over the information that they and their children have access to. In sharp contrast to older media, government content regulation is simply not necessary in order to shield children from possibly inappropriate information. Any legislative action in this are must identify ways to promote greater parental and user control. As drafted, the proposal before us suggests possible FCC rulemaking on this issue, but is no guaranty that the Commission would take this course. Instead of just passing this critical question off to a regulatory body, Congress must

identify both legal and voluntary means to encourage the development of more and more flexible and accessible user control techniques.

Interactive media such as the Internet, commercial online services, and interactive television networks, are, by nature, distinctly different from traditional broadcast and television mass media. Interactive media does not suffer from a scarcity of capacity, nor does it assault an audiance of captive viewers. Most importantly, interactive media offers users tremendous control over the content that they and their children receive. The Exon/Coats proposal completely fails to account for these unique aspects of interactive media. As House of Representatives begins to consider this and other proposals to regulate content on the Internet, CDT will continue to fight the Exon/Coats proposal, and will work to find alternative prolicy solutions which preserve the First Amendment an the free flow of information in cyberspace.

Center for Democracy and Technology
Jerry Berman <jberman@cdt.org>
Daniel Weitzner <djw@cdt.org>

+1.202.637.9800

---

(2) TEXT OF THE STATUTE WITH PROPOSED AMENDMENT

TITLE 47. TELEGRAPHS, TELEPHONES, AND RADIOTELEGRAPHS
CHAPTER 5. WIRE OR RADIO COMMUNICATION
COMMON CARRIERS

47 USCS | 223 (1992)

| 223. Obscene or harassing telephone calls in the District of Columbia or in interstate or foreign communications

Strike all of current Section (a) and insert the following:

(a) Whoever --

(1) in the District of Columbia or in interstate or foreign communications

(A) by means of telecommunications device knowingly --

(i) makes, creates, or solicits, and
(ii) initiates the transmission of,

any comment, request, suggestion, proposal, image, or other communication which is obscene, lewd, lascivious, filthy, or indecent, with intent to annoy, abuse, threaten, or harass another person;

(B) makes a telephone call or utilizes a telecommunications device, whether or not conversation or communication ensues, without disclosing his identity and with intent to annoy, abuse, threaten, or harass any person at the called number or who receives the communication;

(C) makes or causes the telephone of another repeatedly or continuously to ring, with intent to harass any person at the called number; or

(D) makes repeated telephone calls or repeatedly initiates communication with a telecommunications device, during which conversation or communication ensues, solely to harass any person at the called number or who receives the communication; or

(2) knowingly permits any telecommunications facility under his control to be used for any activity prohibited by paragraph (1) with the intent that it be used for such activity,

shall be fined not more than $100,000 or imprisoned not more than two years, or both._

NO CHANGE TO THE DIAL-A-PORN SECTIONS (B) AND (C)

(NOTE: BILL ADDS NEW SECTIONS (D) - (J))

(d) Whoever--

(1) knowingly within the United States or in foreign communications with the United States by means of telecommunications device makes or makes available any obscene communication in any form including any comment, request, suggestion, proposal, image, regardless of whether the maker of such communication placed the call or initiated the communications; or

(2) knowingly permits any telecommunications facility under such person's control to be used for an activity prohibited by subsection (d)(1) with the intent that it be used for such activity;

shall be fined not more than $100,000 or imprisoned not more than two years or both.

(e) Whoever--

(1) knowingly within the United States or in foreign communications with the United States by means of telecommunications device makes or makes available any indecent comment, request, suggestion, proposal, image to any person under 18 years of age regardless of whether the maker of such communication placed the call or initiated the communication; or

(2) knowingly permits any telecommunications facility under such person's control to be used for an activity prohibited by paragraph (1) with the intent that it be used for such activity,

shall be fined not more than $100,000 or imprisoned not more than two years or both.

(f) Defenses to the subsections (a), (d), and (e), restrictions on access, judicial remedies respecting restrictions for persons providing information services and access to information services--

(1) No person shall be held to have violated subsections (a), (d), or (e) solely for providing access or connection to or from a facility, system, or network over which that person has no control, including related capabilities which are incidental to providing access or connection. This subsection shall not be applicatable to an individual who is owned or controlled by, or a conspirator with, an entity actively involved in the creation, editing or knowing distribution of communications which violate this section.

(2) No employer shall be held liable under this section for the actions of an employee or agent unless the employee's or agent's conduct is within the scope of his employment or agency and the employer has knowledge of, authorizes, or ratifies the employee's or agent's conduct.

(3) It is a defense to prosecution under subsection (a), (d)(2), or (e) that a person has taken reasonable, effective and appropriate actions in good faith to restrict or prevent the transmission of, or access to a communication specified in such subsections, or complied with procedures as the Commission may prescribe in furtherance of this section. Until such regulations become effective, it is a defense to prosecution that the person has complied with the procedures prescribed by regulation pursuant to subsection (b)(3). Nothing in this subsection shall be construed to treat enhanced information services as common carriage.

(4) No cause of action may be brought in any court or any administrative agency against any person on account of any action which in not in violation of any law punishable by criminal penalty, which activity the person has taken in good faith to implement a defense authorized under this section or \ otherwise to restrict or prevent the transmission of, or access to, a communication specified in this section.

(g) no state or local government may impose any liability for commercial activities or actions by commercial entities in connection with an activity or action which constitutes a violation described in subsection (a)(2), (d)(2), or (e)(2) that is inconsistent with the treatment of those activities or actions under this section provided, however, that nothin herein shall preclude any State or local government from enacting and enforcing complementary oversight, liability, and regulatory systems, procedures, and requirements so long as such systems, procedures, and requirements govern only intrastate services and do not result

in the imposition of inconsistent rights, duties or obligations on the provision of interstate services. Nothing in this subsection shall preclude any State or local government from governing conduct not covered by this section.

(h) Nothing in subsection (a), (d), (e), or (f) or in the defenses to prosecution under (a), (d), or (e) shall be construed to affect or limit the application or enforcement of any other Federal law.

(i) The use of the term 'telecommunications device' in this section shall not impose new obligations on (one-way) broadcast radio or (one-way) broadcast television operators licensed by the Commission or (one-way) cable services registered with the Federal Communications Commission and covered by obscenity and indecency provisions elsewhere in this Act.

(j) Within two years from the date of enactment and every two years thereafter, the Commission shall report on the effectiveness of this section.

---

(3) About The Center For Democracy And Technology/Contacting Us

The Center for Democracy and Technology is a non-profit public interest organization. The Center's mission is to develop and advocate public policies that advance constitutional civil liberties and democratic values in new computer and communications technologies.

Contacting us:

To subscribe to CDT's news distribution list (to receive future Policy Posts directly), send email to <cdt-lists@cdt.org> with a subject of 'subscribe policy posts'.

NOTE TO THOSE WHO HAVE ALREADY REQUESTED TO BE ADDED TO CDT's DISTRIBUTION LIST: We are still working to build our listserv -- you will begin receiving Policy Posts on this list very soon. We appreciate your patience!

General information on CDT can be obtained by sending mail to info@cdt.org

World-Wide-Web:

http://www.cdt.org/

ftp:

ftp://ftp.cdt.org/pub/cdt/

snail mail:

Center For Democracy and Technology
1001 G Street, NW Suite 700 East
Washington, DC 20001
voice: +1.202.637.9800
fax: +1.202.637.9800
###

POLICY POST

June 21, 1995
Number 20

CENTER FOR DEMOCRACY AND TECHNOLOGY

A briefing on public policy issues affecting civil liberties online
---
CDT POLICY POST Number 20 June 21, 1995

CONTENTS: (1) CDT PRAISES SPEAKER GINGRICH'S OPPOSITION TO EXON/COATS INTERNET CENSORSHIP BILL

PRESS RELEASE -- For Immediate Release
June 21, 1995
Contact: the Center for Democracy and Technology at +1.202.637.9800

CENTER FOR DEMOCRACY AND TECHNOLOGY PRAISES SPEAKER GINGRICH'S OPPOSITION TO EXON/COATS INTERNET CENSORSHIP BILL.

In a move that is a boon for freedom of speech rights for Internet users, Speaker of the House Newt Gingrich has condemned the Exon/Coats "Communications Decency Act" as a "clear violation of free speech and ... a violation of the right of adults to communicate with each other."

"Speaker Gingrich has demonstrated that he understands the unique nature of interactive media such as the Internet," said CDT Executive Director Jerry Berman. "Gingrich's leadship on this issue will assure that new interactive media will be free to grow without unproductive government intrusion, and that the First Amendment rights of users will be protected."

The statement from the Republican leader came on the same day that Rep. Chris Cox (R-CA) and Rep. Ron Wyden (D-OR) announced that they are developing a different approach to the problem of children's access to controversial material on the Internet. Cox and Wyden say that they seek to encourage the development of blocking and filtering technologies that empower parents to screen the material to which their children have access. At the same time, they hope to keep the growing Internet free from intrusive and ineffective regulation by the Federal Communications Commission.

"Along with the Speaker, Congessmen Cox and Wyden know that federal content censorship such as has existed in radio and television mass media will not

be effective at protecting children," said Daniel Weitzner, CDT Deputy Director. "In the decentralized, global Internet environment, we must rely on user control technology to enable users and parents to determine for themselves the information that they and their children receive."

The Exon Internet censorship bill was strongly opposed in the Senate by Senator Patrick Leahy (D-VT) and Senator Russell Feingold (D-WI). The Exon/Coats bill was approved, however, by the Senate last week and is still awaiting House action.

Gingrich made his remarks (attached below) last night on a national television show, the Progress Report carried on National Empowerment Television during a discussion with Rep. Bob Walker (R-PA) and Progress and Freedom Foundation Chairman Jay Keyworth.

Gingrich said:

"I think that the Amendment you referred to by Senator Exon in the Senate will have no real meaning and have no real impact and in fact I don't think will survive. It is clearly a violation of free speech and it's a violation of the right of adults to communicate with each other. I don't agree with it and I don't think it is a serious way to discuss a serious issue, which is, how do you maintain the right of free speech for adults while also protecting children in a medium which is available to both? That's also frankly a problem with television and radio, and it's something that we have to wrestle with in a calm and mature way as a society. I think by offering a very badly thought out and not very productive amendment, if anything, that put the debate back a step."

The Center for Democracy and Technology is a non-profit public interest organization. The Center's mission is to develop and advocate public policies that advance constitutional civil liberties and democratic values in new computer and communications technologies.

POLICY POST

July 6, 1995
Number 21

CENTER FOR DEMOCRACY AND TECHNOLOGY

A briefing on public policy issues affecting civil liberties online
---
CDT POLICY POST Number 21 July 6, 1995

CONTENTS: (1) SENATE HEALTH BILL WILL EXPOSE PRIVATE HEALTH RECORDS
(2) ANALYSIS OF 'HEALTH INFORMATION MODERNIZATION AND SECURITY ACT (S. 872)
(3) WHAT YOU CAN DO
(4) ABOUT CDT/CONTACTING US

---

1) BOND HEALTH BILL (S 872) WILL EXPOSE PRIVATE HEALTH RECORDS TO UNAUTHORIZED ACCESS

The "Health Information Modernization and Security Act" (S. 872), introduced in May by Senator Bond (R-MO), poses a serious threat to individual privacy by encouraging the development of health information systems that will expose sensitive personal information to unauthorized use and access. The Bond bill does not adequately address the threats to individual privacy presented by the use of such systems.

CDT urges Congress to pass legislation such as the Fair Health Information Practices Act (H.R. 435) introduced in the House by Gary Condit (D-CA). We urge Senator Bond to amend his proposal to incorporate the comprehensive privacy protections set out in the Condit bill.

Currently there is no comprehensive federal law that protects the confidentiality of personal information that individuals divulge during encounters with the health care industry. Yet most individuals consider information on their health to be the most sensitive information about themselves and to be the information most in need of privacy protection. The lack of strong uniform privacy protection for personal health information has left individuals vulnerable to privacy violations in a paper-based world.

However, the threats to privacy posed by the computerization of personal

health information without appropriate privacy policies and technological mechanisms to control the collection, use, access and disclosure, will make such information more vulnerable to abuse than ever before.

The traditional barriers of location and time disappear in the age of computerization. With birth to death dossiers on each American on line the potential for multiple simultaneous access from various locations exists. The locked file cabinet that traditionally protected medical information from prying eyes must be reinvented for the age of automation. Legislation to protect the privacy of health information is urgently needed.

As health care reform came to a halt at the end of the 103rd Congress, a piece of health care reform legislation that received support from Democrats, Republicans, health providers, health insurers, and privacy advocates was the Fair Health Information Practices Act (introduced by Senator Pat Leahy (D-VT) and Representative Condit. The bill was coupled with an earlier version of Bond's Health Information Modernization Bill. In fact, the privacy protections for health information found in these proposals were fleshed out versions of language contained in every major piece of health care reform legislation in Congress. Protecting the privacy and confidentiality of health information is one of the issues on which broad consensus was reached during the health care debate last year.

Without a detailed privacy section, the Health Information Modernization and Security Act harkens back to provisions in President Clinton's Health Security Act that received widespread ridicule. Like the Administration's Health Security Act, Senator Bond's proposal fails to fully address the confidentiality of personal health information.

The Health Information Modernization and Security Act fails to incorporate privacy and security standards into the legislation. It directs the Secretary of Health and Human Services to establish standards for the implementation of privacy and security within eighteen months of enactment.

The lack of privacy, confidentiality and security provisions within the Act is disturbing, since a goal of the bill is "encouraging the development of a health information network through the establishment of standards and requirements for the electronic transmission of certain health information." The Act would greatly increase the ease with which information is accessed, compiled, exchanged and manipulated. The failings of this bifurcated approach to policy and technology were readily apparent to the Administration, Congress, privacy advocates and the private sector in 1994. If Congress advocates a move to automated record keeping, it must simultaneously protect the sensitive information on individuals that will be stored and transmitted by these systems. Before the government accelerates or mandates computerization in the health care field, it is crucial comprehensive privacy protections for health information be established.

During last Congress there was consensus that health information systems could not be designed and constructed without enforceable privacy rules in place. It is neither reasonable nor rational to design a system knowing that the sensitive information each American would be asked to entrust would be largely unprotected from misuse and abuse, and that the failure to address privacy up front would likely lead to a complete system redesign or overhaul years later at an increased cost.

We urge Senator Bond and Congress to ensure that personal health information is protected by strong enforceable privacy protections.

FOR MORE INFORMATION CONTACT:

Janlori Goldman, Deputy Director
Deirdre Mulligan, Staff Counsel

Center for Democracy and Technology +1.202.637.9800

---

2) ANALYSIS OF BOND S. 872

General Provisions: Titles I & II

The objective of the proposal is to encourage the development of a health information network through the establishment of standards and requirements for the electronic transmission of certain health information. (Sec. 101) The Secretary of HHS is given responsibility for adopting standards for data elements and transactions, but is to be guided by current practice and by standards developed or modified by a standards setting organization (this is likely to be the American National Standard Institute - ANSI). (Sec. 1172) Sec. 1174 requires that the Secretary adopt standards relating to the information transactions, data elements and security and privacy within 18 months of enactment.

The Secretary is to adopt uniform standards to increase the electronic availability of "financial and administrative transactions: claims or equivalent encounter information, claims attachments, enrollment and disenrollment, eligibility, payment and remittance advice, premium payments, first report of injury, claims status, referral certification and authorization," and "other transactions determined appropriate by the Secretary consistent with the goals of improving the operation of the health care systems and reducing administrative costs." (Sec. 1173(a)(1)).

In addition, the Secretary is to adopt a unique health identifier for each individual. (Sec. 1174(b)(1)). Sec. 1177 sets penalties for use of the unique health identifier that are not authorized by the Secretary.

The Secretary is to promulgate regulations specifying procedures for the electronic transmission and authentication of signatures that will meet current federal and state written signature requirements, "pen & quill" laws. (Sec. 1173(d)1)

Privacy and Security Standards:

Section 1172(b)(1) requires each person who "maintains or transmits health information or data elements that are subject to this Act" to maintain reasonable and appropriate administrative, technical and physical safeguards to ensure integrity and confidentiality and to protect against reasonably anticipated threats or hazards and unauthorized uses and disclosures.

Section 1174(b) gives the Secretary one and one-half years post enactment to establish the standards for implementing the privacy standards.

Penalties for Wrongful Disclosure of Individually Identifiable Health Information

Under Section 1177, individuals who violate the privacy standards, which govern obtaining or disclosing individually identifiable health information, established by the Secretary, may be fined up to $50,000 and imprisoned up to 1 year, or both. If the offense is committed under false pretenses the fine can be up to $100,000 and the sentence up to 5 years. If the offense is committed with the intent to sell, transfer, use for commercial advantage or personal gain, or use to maliciously harm the individual, the fine may be up to $250,000 and the sentence up to 10 years.

Preemption

The Act would preempt contrary provisions of State laws, including "requirements or standards that are more stringent than the requirements or standards under the Act, except: 1) where the requirement is more stringent with respect to electronic transmissions of financial or administrative transactions from providers to plans and incorporates standards adopted under the bill; 2) more stringent with respect to the privacy of individually identifiable health information; of 3) is an already enacted provisions governing the coordination of benefits; or 4) in the Secretary's judgment, is necessary to curtail fraud and abuse. (Sec. 1178) The Act does not invalidate or curtail public health reporting laws. (Sec. 1178(b)).

Health Information Advisory Committee

Section 1179 establishes a Health Information Advisory Committee (15 members) to advise and assist the Secretary. The Committee is directed to study the issues of uniform standards and electronic exchange and report to the Secretary within four years of enactment. The Committee is to report annually on compliance with the act. The report will address compliance with privacy and security standards among other issues.

Standards for Patient Medical Record Information

Under Section 1180, within four to six years, the Secretary shall

recommend a plan for developing and implementing uniform data standards for patient medical record information and the electronic exchange of such information.

Grants for Demonstration Projects

The Secretary is given the right to make grants for demonstration projects aimed at promoting the development and use of electronically integrated, community-based clinical information systems and computerized patient medical records.

---

3) WHAT YOU CAN DO

There is currently a companion bill in the House of Representatives, H.R. 1766, the Health Information Modernization and Security Act, introduced by Representative Thomas Sawyer (D-OH) and Representative David Hobson (R-OH). This bill is very similar to Senator Bond's bill. All concerns held by the Center for Democracy and Technology for Senator Bond's bill are also held for H.R. 1766.

We urge you to contact Senator Bond (202) 224-5721 to voice your concern over S. 872, Health Information Modernization and Security Act, and Representatives Hobson (202) 225-4324 and Sawyer (202) 225-5231 over the House bill H.R. 1766, Health Information Modernization and Security Act.

---

(4) ABOUT THE CENTER FOR DEMOCRACY AND TECHNOLOGY/CONTACTING US

The Center for Democracy and Technology is a non-profit public interest organization. The Center's mission is to develop and advocate public policies that advance constitutional civil liberties and democratic values in new computer and communications technologies.

Contacting us:

General information on CDT can be obtained by sending mail to:

info@cdt.org

World-Wide-Web:

http://www.cdt.org/

ftp:

ftp://ftp.cdt.org/pub/cdt/

snail mail:

Center For Democracy and Technology
1001 G Street, NW Suite 700 East
Washington, DC 20001

voice: +1.202.637.9800
fax: +1.202.637.0968

###

POLICY POST

July 26, 1995
Number 22

CENTER FOR DEMOCRACY AND TECHNOLOGY

A briefing on public policy issues affecting civil liberties online
---
CDT POLICY POST Number 22 July 26, 1995

CONTENTS: (1) Senate Judiciary Committee Holds Cyberporn Hearing
(2) House Science Subcommittees Hold Hearing to Explore
Parental Control Technology -- Law Enforcement Officials
Say Exon CDA is Wrong Approach
(3) Subcribe To The CDT Policy Post Distribution List
(4) About CDT, Contacting US

---

(1) SENATE JUDICIARY COMMITTEE HOLDS CYBERPORN HEARING

SUMMARY

On Monday July 24, 1995 the Senate Judiciary Committee held the first ever hearing on the issue of children's access to inappropriate material on the Internet. The principal focus of the hearing was to discuss Senator Grassley's "Protection of Children from Computer Pornography Act of 1995" (S. 892). CDT Executive Director Jerry Berman testified before the panel.

Senator Grassley (R-IA) deserves praise for holding the first Congressional hearing on this important issue. In addition, both Senator Grassley and Senator Leahy took great pains to ensure that both sides of the issue were represented. Although CDT may disagree with Senator Grassley's approach, we believe that this hearing represented an essential step towards advancing the dialogue on what has become an over-hyped and dramatically misunderstood issue.

Senator Grassley's legislation, which has been co-sponsored by several other prominent members such as Dole (R-KS), Hatch (R-UT), and Thurmond (R-SC), would impose criminal penalties on a service provider that "knowingly" transmits indecent material to a minor, or who "willfully" permits its network to be used to transmit indecent material to a minor (S. 892, Sec (b)(2) & (b)(3)).

Two important points emerged from the testimony:

1. Current law prohibits the distribution of obscenity and child pornography, as well as online stalking and solicitation of minors. As troubling and disturbing as some of the testimony was, no evidence was presented that there are gaps in current law which would be filled by the Grassley legislation.

2. Serious questions exist as to the constitutionality of the Grassley Bill. Although Senator Grassley has repeatedly stated that his bill is narrowly drawn and targets only the bad actors, no evidence was presented to establish that a court would not interpret the statute more broadly, resulting in a complete ban on constitutionally protected speech online.

WITNESSES

Witnesses testifying before the panel included:

Donnelle Gruff, a 15 year old Florida girl described as a victim of an online stalker,
P--- S---, a mother of two from Baltimore MD and volunteer for Enough Is Enough
Dr. Susan Elliot, a mother from McLean VA

Bill Burrington, Assistant General Counsel, America Online
Barry Crimmins, a children's rights advocate
Stephen Balkam, Executive Director, Recreational Software Advisory Counsel

Jerry Berman, Executive Director, Center for Democracy and Technology
Michael S. Hart, Executive Director of Project Gutteberg, Professor of Electronic Texts, Illinois Benedictine College
Dee Jepsen, Enough Is Enough (an anti-pornography group)

DOES THE GRASSLEY BILL PROTECT CHILDREN?

The testimony of 15 year old Donnelle Gruff focused on her experience as the victim of a stalker, while Dr. Elliot and Ms. S---, two mothers of young children, described how their children had used commercial online services to access files they deemed inappropriate.

Donnelle Gruff testified that she had been harassed and stalked by the sysop of a Florida BBS she had visited. The sysop had obtained her name, age, and address from her records and reportedly stalked Gruff while she was at home.

During questioning however, Gruff's step-father told Senator Patrick Leahy (D-VT) that Florida law enforcement officials were currently investigating the case, and that they had given no indication that current law is insufficient with respect to prosecuting such cases. Senator Leahy noted that, as difficult and disturbing as Gruff's case is, it illustrates a need for additional law enforcement resources and

education, but is not an issue of gaps in current federal or state laws. Senator Leahy mentioned similar recent prosecutions in Florida, and noted that the Grassley legislation does not explicitly prohibit online stalking of minors.

In addition, Senator Leahy questioned whether government content restrictions would be an effective solution to protecting children online. "I hear a lot of rhetoric (from Congress) about getting government out of our lives, but here it seems as if the rhetoric is a little off of reality. Parents, not the government, should make the choices" about what their children should be permitted to access.

Both Dr. Elliot and Ms. S--- testified that their children had stumbled across material while surfing the Internet that they, as parents, felt should not be accessible to children. Both described how their children had accessed "pornographic" images, and had been propositioned for "cybersex" while visiting a chat room on a commercial online service. In addition, Dr. Elliot described some of the images as representing 'bestiality and sodomy'.

Barry Crimmins, a child protection advocate, testified that he has found numerous images of child pornography on America Online. Crimmins accused AOL of neglecting to adequately police its network. When questioned by Senator Leahy, Crimmins acknowledged that the distribution of child pornography and stalking or solicitation of minors is prohibited under current law. Crimmins added that while he thought the commercial online service should do more to remove such material, he believes that more vigorous enforcement of existing law would help to address his concerns.

WHAT IS THE SCOPE OF THE ISSUE -- IS CURRENT LAW SUFFICIENT?

Often in the course of the debate on this issue, the term "pornographic" is assumed to be interchangeable with both "indecency" and "obscenity". However as Senator Russ Feingold (D-WI) noted, "pornography" has no legal standing, and when legislating in this area Congress must be careful to avoid confusing these legal distinctions.

In determining what material would be considered illegal under current law, the distinction between "obscene" and "indecent" material must be made completely clear. When pressed by Senator Feingold, Dr. Elliot agreed that precise definitions are important, but argued that the files that her child downloaded from the Internet that depicted bestiality and sodomy that would be, "obscene by any standard".

Images of bestiality and sodomy, as Dr. Elliot described, would be considered obscene in virtually every community in the United States, and hence are illegal under current law. Though it raises difficult jurisdictional questions, obscenity has been clearly defined by the Courts. Moreover, trafficking in obscenity (18 USC Sec 1462, 1464, 1466) as well as child pornography (18 USC Sec 2252) have been successfully applied to punish conduct on computer networks. As Senator Leahy pointed out in his statement, the Justice Department is currently prosecuting cases involving material similar to that described by Dr. Elliot.

Indecent material, on the other hand, is constitutionally protected and is much more difficult to define. The most common understanding of what constitutes indecent material includes the 7 dirty words, images of nudity, and other suggestive material. Moreover, the Supreme Court has ruled that any attempts by government to restrict access to indecent material must be accomplished in the "least restrictive means", and the determination of this standard is entirely dependent on the medium (see Sable Communications v. FCC, 492 US 115; 109 S.Ct. 2829; 106 L.Ed. 2d 93 (1989).

Some of the material described by the witnesses would be considered obscene, and hence is already prohibited under current law. Other examples, including Ms. S---'s description of her daughter being propositioned for "cybersex", would likely not be considered obscene.

Senator Feingold urged the committee to carefully consider the distinctions between "obscene" and "indecent" speech, and urged his colleagues to "exercise caution and restraint."

How broadly should we define indecency, Feingold asked Dr. Elliot, "Where should we draw the line? Should we prohibit Playboy? swearing? The Catcher In The Rye? What about a discussion forum about how to avoid getting AIDS?".

Because technologies currently exist to screen out messages such as those described by Ms. S---, it is unlikely that a broad prohibition on such messages would pass constitutional muster. In this case, Congress must look to other, less restrictive methods of preventing children from having access to such materials -- including promoting the development and availability of user control technologies.

CONSTITUTIONAL ISSUES

Throughout the hearing, Senator Grassley stated that his legislation is carefully crafted and narrowly drawn in order to preserve the First Amendment rights of adults while protecting children from inappropriate material. Grassley stated that his bill would hold an online service provider liable only in cases where they "knowingly" allow their network to be used to transmit indecent material to a minor or "willfully" allow an individual to use their network to do so.

However, as CDT's Jerry Berman and America Online's Bill Burrington argued the wording of the statute and the variety of possible interpretations could lead to severe chilling effect on the free flow of legitimate information in cyberspace and force online service providers to limit or remove certain areas of their service.

BROAD KNOWLEDGE REQUIREMENT

The scope of the "knowing" standard in the Grassley bill is an issue of some dispute. Senator Grassley and his staff maintain that it is intended to apply narrowly, but no evidence was presented that demonstrated why a court would apply a narrow interpretation.

Berman cautioned that because of this uncertainty, online service providers would be forced to rely on the broadest possible interpretation of the statute in order to avoid liability, resulting in a severe chilling effect on all online communications:

"The threat of a broad interpretation of this new statute would compel all who provide access to the Internet to restrict all public discussion areas and public information sources from subscribers, unless they prove that they are over the age of eighteen. Under this statute, a service provider could not even provide Internet access to a minor with the approval of the child's parent. Since every online service provider would have to similarly restrict access to minors, this proposed statute would create two separate Internets, one for children and one for adults."

America Online's Bill Burrington agreed, stating that the potential for a broad interpretation of the statute would compel AOL and other online service providers to adhere to the broadest possible reading in order to avoid potential liability. Burrington argued that would force AOL to shut down many parts of its service and place providers in the unenviable position of national censor.

"Constitutional guarantees of free speech and press should be cautiously guarded," Burrington stated, "The online service provider industry should be encouraged to provide voluntary editorial control over its service and to continue its research and development of parental empowerment technology tools. This industry should not be cast in the role of national censor, determining which information may be fit for children, but nonetheless subject to criminal liability if it guesses incorrectly in any given instance."

Senator Dewine (R-OH) asked several questions of many of the witnesses, and expressed concerne about the potential for an overly board interpretation of the knowledge standard.

BROAD INTERPRETATION OF 'INDECENCY'

As addressed earlier, a precise definition of 'indecent' speech has never been firmly established, and whether material would be considered indecent depends largely on the nature of the medium it is communicated through. Because of this, and because under the Grassley bill carriers would be liable for transmitting indecent speech, carriers would be forced to adhere to the broadest, most inclusive definition of indecency. This would include, among other things, the 7 dirty words, description of genitalia, nudity, and other material which is protected in other media.

This issue was raised by Michael Hart, Executive Director of Project Gutteberg, who stressed that broad restrictions on indecency would prevent people from enjoying serious works of fiction on the Internet. Project Gutteberg makes electronic texts of books available on the Internet. Hart stated, with great emotion, that the proposed indecency restrictions contemplated by the Grassley bill would force him to remove

some of Shakespeare's plays, The Catcher In The Rye, Lady Chatterly's Lover, Alice in Wonderland, and other books which have been classified as indecent in some parts of the United States. Although such an effect may not be intended by the drafters of the Grassley legislation, no evidence was offered at the hearing to counter Mr. Hart's concerns.

EXON vs. BERMAN

CDT's Jerry Berman urged the Committee to act cautiously before voting to further restrict First Amendment guarantees of freedom of speech. Berman urged the Senate to fulfill its traditional role as the "deliberative body", and to carefully consider the implications before enacting broad new statutes to cover new media. Referring to both the Exon CDA and the Grassley bill, Berman stressed that the country would be better served if the Senate did not enact legislation simply to "provide the illusion that the United States Senate could do something in this area".

This remark drew a sharp rebuttal from Senator Exon, who, though not a member of the Judiciary Committee, sat in on the hearing on the invitation of Senator Grassley. Exon defended his bill and accused CDT and others of launching "viscous attacks" against him and his legislation. Berman was not given a chance to respond.

"We are concerned about the situation", Exon argued, yet "we are viscously attacked for trying to have a rational discussion. We don't want to create a false sense of security [but] we have a responsibility to protect children". In addition, Exon dismissed parental control technologies as too little too late, arguing that "for every block there is a way around that block", and that such technologies may not be available in every home, allowing children to access inappropriate material at the homes of neighbors who may not employ such tools.

WHAT WAS LEARNED?

Although the hearing did illustrate that sexually explicit material can be found on the Internet, no substantial evidence was presented to indicate that law enforcement is currently unable to prosecute violations of obscenity, child pornography, stalking, or child solicitation laws. Moreover, although Senator Grassley intends his legislation to be narrow, serious questions were raised about whether other, more board interpretations are possible.

In our opinion, the hearing illustrated that current law is sufficient to prosecute those who stalk or solicit children online, and that complex constitutional issues are raised by congressional attempts to restrict indecent material on the Internet.

PATHS TO RELEVANT DOCUMENTS

Testimony is available for most of the witnesses from CDT's Communications Decency Act Issues page:

URL:http://www.cdt.org/speech/cda/950724list.html

or from our ftp archive:

URL:ftp://ftp.cdt.org/pub/cdt/policy/freespeech

---

(2) HOUSE SCIENCE SUBCOMMITTEE HOLDS 'PARENTAL CONTROL TECHNOLOGY' HEARING

Two subcommittees of the House Science Committee held a joint hearing today (July 26, 1995) on the availability of parental control technologies to prevent children from accessing inappropriate material on the Internet. The hearing, held by the Subcommittee on Basic Research, Chaired by Rep. Schiff (R-NM) and the Subcommittee on Technology, Chaired by Rep. Morella (R-FL) provided an important counter-balance to Monday's Senate Judiciary Committee Hearing.

Witnesses testifying before the committee included:

Witnesses Demonstrating Technology Solutions

Tony Rutkowski, Executive Director of the Internet Society
Ann Duvall, President of SurfWatch Software
Steve Heaton, General Counsel and Secretary, Compuserve

Law Enforcement Witnesses

Kevin Manson, Federal Law Enforcement Training Center
Mike Geraghty, Trooper, New Jersey State Police
Lee Hollander, Assistant States Attorney, Naples Florida

LAW ENFORCEMENT OFFICIALS SAY CURRENT LAW SUFFICIENT, EXON BILL FLAWED

Today's hearing marked the first time law enforcement officials have testified on the issue of children's access to inappropriate material on the Internet. All three law enforcement witnesses agreed that, in their experience, current law is sufficient to prosecute online stalking, solicitation of minors, and the distribution of pornography and child pornography. All three said that they are vigorously prosecuting such cases.

Instead of enacting new law, New Jersey State Trooper Mike Geraghty said that protecting children is "a matter of training law enforcement officers, prosecutors, lawyers and judges about how to enforce existing laws [with respect to computer networks]. The laws are good, we have to learn how to enforce them".

The three law enforcement witnesses further argued that the Senate-passed Exon/Coats Communications Decency Act is the wrong approach to addressing an issue that is already covered under existing law. "I have several problems with the Exon bill as a prosecutor, both in terms of

its practical enforcement and its constitutionality" said Florida Assistant States Attorney Hollander said.

TRANSACTIONAL PRIVACY PROTECTIONS CRITICIZED

In an slightly unrelated asside, Florida Assistant States Attorney Lee Hollander criticized privacy protections for online transactional information as a hindrance to law enforcement.

As part of last years Digital Telephony legislation, the standard for law enforcement access to online transactional records (logs that indicate what files an individual accessed from online archives and electronic mail transactions) was raised from a requirement of a mere subpoena to a court order from a judge based on the showing of "specific and articulable facts" that such records are "relevant and material to an ongoing criminal investigation". The higher standard was widely seen as a victory for online privacy.

In response to a question of what Congress could do to help aid enforcement of existing law, Hollander noted that the higher standard for online transactional records adds an additional burden to law enforcement investigations. Calling it part of a "ballance between privacy and law enforcement", Hollander did not suggest that Congress should repeal the court order requirement, only that it made prosecutions more difficult (NOTE: Members of CDT staff worked closely on this issue, and consider the court order standard to be a tremendous victory for online privacy).

EXON CDA CONDEMNED BY ALL

Condemnation of the Senate-passed CDA was not limited to the law enforcement witnesses. Not a single member of the Subcommittee stated support for the CDA, and all expressed concern that the issue had not received sufficient public consideration by Congress.

Chairwoman Morella stressed that Congress should consider technological options to empower parents to exercise control over what their children access online before rushing to enact new laws. Rep. Geren (D-TX) expressed concern about the First Amendment implications of the CDA. Rep. Vern Elhers (R-MI) stated that he would "oppose bills that make network access providers (legally) responsible for the content they carry". In what was perhaps the strongest condemnation of the Senate-passed Communications Decency Act, Rep. Zoe Loefgren (D-CA) said, "While well intentioned, the Exon bill a totally wrong approach and a complete misunderstanding of the Technology."

PARENTAL CONTROL TECHNOLOGY IS THE ONLY EFFECTIVE SOLUTION

Internet Society Executive Director Tony Rutkowski provided Committee members with a basic overview of the Internet and noted that the Internet Society (ISOC) and Internet Engineering Task Force (IETF) are currently looking at content tagging and other voluntary rating systems for future Internet protocols. Rutkowski stressed that centralized,

command and control style content restrictions would be ineffective in the global, distributed network environment of the Internet. Rutkowski further noted that objectionable material constitutes a minuscule amount (less than .05%) of the total traffic on the network.

Because of the global reach of the Internet and the millions of potential content providers, Rutkowski argued, the only effective means of addressing the availability of inappropriate material is to provide user control applications to empower parents to block and filter what the and their children access.

SurfWatch President Ann Duvall, demonstrated SurfWatch, and described the product as "just one example of the computer industry responding to needs created by the explosive growth of technology". Duvall stressed that the industry is developing solutions which are simple to use, inexpensive, and empower parents to make their own choices about what they or their children should see.

Expressing concern about legislative efforts to control content online, Duvall noted that 30% of the sites blocked by SurfWatch reside outside the United States. "There is not a simple, national solution to the problem of children accessing inappropriate material on the Internet. Excessive government regulations might jeopardize private sector opportunities. SurfWatch firmly believes that the technology industry can and must respond to these socio-technological issues. We also affirm that parents must be involved in any solution"

Compuserve General Counsel Steve Heaton agreed with some of the Committee members that parents have a right to be concerned about the availability of certain material on the Internet, but stressed that government solutions are no substitute for empowering users. Heaton described some of the current parental control technology, and outlined Compuserve's plans to develop KidNet, an interactive service designed specifically for kids.

Heaton cautioned against overly broad attempts to regulate content on the Internet and other interactive communications service: "The cyber community, made up of hundreds of thousands of computers distributed across the globe, is truly a world without borders. Directly regulating cyberspace -- history's only true functioning anarchy -- may prove impossible. This makes it imperative that laws focus on individual responsibility and that education and empowerment among users and concerned parents be emphasized."

PATHS TO RELEVANT DOCUMENTS

Testimony from the Science Committe hearing will be available on CDT's Communications Decency Act Issues Page beginning Friday July 28.

URL:http://www.cdt.org/cda.html

It will also be available on our ftp site

URL://ftp.cdt.org/pub/cdt/policy/freespeech

---
(3) How To Subcribe To The CDT Policy Post Distribution List

CDT Policy Posts, which is what you have just finished reading, is the regular news publication of the Center For Democracy and Technology. CDT Policy Posts are designed to keep you informed on developments in public policy issues affecting civil liberties online.

SUBSCRIPTION INFORMAITON

1. SUBSCRIBING TO THE LIST

To subscibe to the Policy Post distribution list, send mail to "Majordomo@cdt.org" with:

subscribe policy-posts

in the body of the message (leave the subject line blank)

2. UNSUBSCRIBING FROM THE LIST

If you ever want to remove yourself from this mailing list, you can send mail to "Majordomo@cdt.org" with the following command in the body of your email message:

unsubscribe policy-posts youremail@local.host (your name)

(leave the subject line blank)

---
(4) ABOUT THE CENTER FOR DEMOCRACY AND TECHNOLOGY/CONTACTING US

The Center for Democracy and Technology is a non-profit public interest organization. The Center's mission is to develop and advocate public policies that advance constitutional civil liberties and democratic values in new computer and communications technologies.

Contacting us:

General information on CDT can be obtained by sending mail to info@cdt.org

World-Wide-Web:

http://www.cdt.org/

ftp:

ftp://ftp.cdt.org/pub/cdt/

snail mail:

Center For Democracy and Technology
1001 G Street, NW Suite 700 East
Washington, DC 20001
voice: +1.202.637.9800
fax: +1.202.637.0968
###

POLICY POST

August 4, 1995
Number 23

CENTER FOR DEMOCRACY AND TECHNOLOGY

A briefing on public policy issues affecting civil liberties online
---
CDT POLICY POST Number 23 August 4, 1995

CONTENTS: (1) House Approves Cox/Wyden 'Internet Freedom' Bill 420 to 4
Major Victory for Cyberspace -- Indecency Statues Remain
A Serious Issue
(2) Subcribe To The CDT Policy Post Distribution List
(3) About CDT, Contacting US

---

(1) HOUSE PASSES COX/WYDEN 'INTERNET FREEDOM' AMENDMENT
MAJOR VICTORY FOR CYBERSPACE -- INDECENCY STATUTES REMAIN A MAJOR ISSUE

By a overwhelming vote of 420 to 4, the US House of Representatives today approved the 'Internet Freedom and Family Empowerment' amendment, sponsored by Reps. Chris Cox (R-CA) and Ron Wyden (D-OR), which would prohibit the federal government from regulating content on the Internet, commercial online services, and other interactive media.

Unlike the Senate-passed Exon/Coats Communications Decency Act (CDA), the Cox/Wyden amendment ensures that individuals and parents can decide for themselves what information they or their children receive. By contrast, the Exon/Coats CDA would grant the Federal Communications Commission (FCC) broad powers to regulate the expression of each and every one of the millions of users of the Internet.

The Cox/Wyden amendment:

Prohibits the FCC from imposing content regulations on the Internet or other interactive media.

Removes disincentives for online service providers to exercise editorial control over their networks and to provide blocking and screening technologies to their uses.

Seeks to create a uniform national policy prohibiting content regulations in interactive media.

CDT believes that the Cox/Wyden amendment is an enlightened approach to addressing the issue of children's access to objectionable material online. Unlike the Senate-passed CDA, the Cox/Wyden approach recognizes that the Internet is a global, decentralized network, with abundant capacity for content and tremendous user control.

House passage of the Cox/Wyden amendment sets the stage for a direct battle between the House and Senate on the issue of government content regulation in interactive media. CDT will work vigorously to ensure that the Cox/Wyden amendment replaces the Exon/Coats CDA in the final version of telecommunications Reform legislation.

NEW UNCONSTITUTIONAL INDECENCY RESTRICTIONS ALSO APPROVED

Although the House vote today significantly advanced freedom of speech on the Internet, the threat of unconstitutional indecency restrictions remains.

In a vote unrelated to the Cox/Wyden amendment, the House also approved changes to federal obscenity laws which would criminalize the transmission of constitutionally protected speech online. These amendments were approved as part of the "Managers Amendment" to the Telecommunications reform bill (HR 1555). Although these amendments are more narrowly drawn than the Exon/Coats CDA or the Grassley/Dole "Protection of Children from Computer Pornography Act (S. 892), they clearly violate the First Amendment and remain an issue of serious concern to CDT.

The new criminal law amendments are opposed by several prominent members of both the House and Senate, including Cox and Wyden. As the bill makes its way through the House/Senate conference committee, CDT will work with Reps. Cox and Wyden, Senator Leahy, and others to:

Remove the unconstitutional indecency restrictions added as part of the "Managers amendment"

Ensure that the Cox/Wyden amendment replaces the Exon/Coats CDA in the final telecommunications reform bill

Clarify that the Cox/Wyden amendment does not affect privacy protections under the Electronic Communications Privacy Act (ECPA)

Strengthen provisions that pre-emption state online censorship laws.

COX/WYDEN AMENDMENT PROTECTS CYBERSPACE FROM GOVERNMENT INTRUSION, RECOGNIZES PARENTAL CONTROL POSSIBILITIES

The Cox/Wyden bill seeks to accomplish four principal objectives:

PROHIBIT FCC CONTENT REGULATION OF THE INTERNET AND INTERACTIVE

COMMUNICATIONS SERVICES.

The bill explicitly prohibits the Federal Communications Commission from imposing or content or other regulations on the Internet or other interactive communications services (Sec 2 (d)).

This provision recognizes that Interactive media is different from traditional mass media (such as broadcast radio and television), and will enshrine in statue strong protections for all content carried on the Internet and other interactive communications services. Instead of relying on government censors to determine what is or is not appropriate for audiences, this provision recognizes that individuals and parents are uniquely qualified to make those judgments.

REMOVE DISINCENTIVES FOR ONLINE SERVICE PROVIDERS TO EXERCISE EDITORIAL CONTROL OVER THEIR NETWORKS AND TO DEPLOY BLOCKING AND SCREENING TECHNOLOGIES FOR THEIR SUBSCRIBERS.

The bill would remove liability for providers of interactive communications services who take good faith steps to restrict access to obscene or indecent materials to minors or provide software or hardware to enable their users to block objectionable material.(Sec 2 (c)) In addition, the bill would overturn the recent court decision (Stratton Oakmont, Inc. v. Prodigy Services Co., N.Y. Sup. Ct. May 24, 1995) which held Prodigy liable for content on its network because the service screens for sexually explicit material and language. Prodigy now faces a $200 million lawsuit.

The bill does not intend to create an obligation for providers to monitor or screen content or to allow violation of Federal privacy statutes (such as the Electronic Communications Privacy Act), although some concerns remain on these points. CDT remains committed to addressing these concerns as the legislation moves to conference, and has been assured by Rep. Cox and Wyden that these issues will be addressed.

PRE-EMPT INCONSISTENT STATE LAWS REGULATING CONTENT ON INTERACTIVE COMMUNICATIONS SERVICES.

The bill seeks to pre-empt States from enforcing inconsistent laws, including restrictions on content available on interactive communications services. (Sec 2 (e)(2))

The actual scope of this preemption remains an issue of some discussion. CDT believes that any legislation in this area MUST contain a strong pre-emption of inconsistent state laws. A patchwork of state laws which impose varying, and in some cases contradictory, obligations on service providers and content providers must be avoided. CDT will work to ensure that the Cox/Wyden bill creates a uniform national policy which prohibits states from imposing content regulations on interactive media.

NO EFFECT ON CRIMINAL LAW.

The bill is not intended to prevent the enforcement of the current dial-a-porn statute or other Federal criminal statutes such as obscenity, child pornography, harassment, etc. (Sec 2 (e)(1))

NET ACTIVISM A CRITICAL FACTOR

When Senator Exon (D-NE) first proposed the CDA in February 1995, the net.community reacted with strong opposition. A coalition of online activist organizations, including CDT, EFF, People for the American Way, EPIC, the ACLU and organized with the Voters Telecommunications Watch (VTW), worked tirelessly over the last six months to mobilize grass roots opposition to the CDA. Through our efforts of generating thousands of phone calls to Congressional offices and an online petition which generated over 100,000 signatures in support of an alternative to the CDA, the net.community was able to demonstrate that we are a political force to be reckoned with.

The net.campaign and public education efforts helped to encourage House Speaker Newt Gingrich (R-GA) to come out against the CDA, and was an important factor in Reps. Cox and Wyden's decision to propose their alternative. As the legislation moves to the conference committee and then on to final passage, the net.community must be prepared to continue to fight to ensure that the new criminal provisions are removed and that the Cox/Wyden amendment is not weakened.

GENESIS OF THE COX/WYDEN AMENDMENT

After the Senate passed the CDA by a vote of 84-16 on June 14, CDT stepped up our efforts to find an alternative which protected the First Amendment and recognized the unique nature of interactive media. Both on our own and through the Interactive Working Group (a group of over 80 public interest organizations and leading computer and communications companies, content providers, and others, coordinated by CDT. The IWG includes the ACLU, People for the American Way, the Progress and Freedom Foundation, America Online, MCI, Compuserve and Prodigy, and many other organizations and corporations), worked directly with Reps. Cox and Wyden to bolster the case that parental control technologies offered an effective alternative to government content regulations.

To this end, the IWG held a demonstration for members of Congress and the press in mid-July to demonstrate parental control feature of products offered by Netscape, SurfWatch, WebTrack, America Online, and Prodigy.

In addition, the IWG issued a comprehensive report reviewing current technology and the state of current laws prohibiting trafficking in obscenity, child pornography, stalking, threats, and other criminal conduct online (this report can be viewed on CDT's web site URL:http://www.cdt.org/iwg/IWGrept.html).

Through these efforts and the efforts of VTW's online coalition, to educate members of the House about the problems with the Exon/CDA and the promise of interactive media, the House today has enacted an

enlightened approach to dealing with children's access to inappropriate material online. Today's vote represents a tremendous victory for the first amendment and the promise of cyberspace.

NEXT STEPS

The House Telecommunications legislation (HR 1555) is expected to pass later today (8/4). The Senate approved similar legislation (S. 652) in June. Both bills now move to a House/Senate Conference Committee where differences will be worked out. The Conference Committee is expected to begin deliberation in early September. Once the Conference Committee agrees on a version of the bill, it will be sent back to both the House and Senate for final approval. This vote is expected to occur before the end of October.

The Internet-censorship provisions of the Senate bill are among the key difference between the House and Senate proposals. However, several key members of the Senate, including Senator Patrick Leahy (D-VT) and Russ Feingold (D-WI) have expressed opposition to the Exon/Coats approach.

CDT will fight vigorously throughout the remainder of this Congress to ensure that the Exon/Coats CDA does not become law. We will also work to remove the new unconstitutional criminal law amendments passed by the House today.

---

(3) How To Subcribe To The CDT Policy Post Distribution List

CDT Policy Posts, which is what you have just finished reading, are the regular news publication of the Center For Democracy and Technology. CDT Policy Posts are designed to keep you informed on developments in public policy issues affecting civil liberties online.

SUBSCRIPTION INFORMAITON

1. SUBSCRIBING TO THE LIST

To subscibe to the policy post distribution list, send mail to "Majordomo@cdt.org" with:

subscribe policy-posts

in the body of the message (leave the subject line blank)

2. UNSUBSCRIBING FROM THE LIST

If you ever want to remove yourself from this mailing list,
you can send mail to "Majordomo@cdt.org" with the following command
in the body of your email message:

unsubscribe policy-posts youremail@local.host (your name)

(leave the subject line blank)

---
(4) ABOUT THE CENTER FOR DEMOCRACY AND TECHNOLOGY/CONTACTING US

The Center for Democracy and Technology is a non-profit public interest organization. The Center's mission is to develop and advocate public policies that advance constitutional civil liberties and democratic values in new computer and communications technologies.

Contacting us:

General information on CDT can be obtained by sending mail to <info@cdt.org>

World-Wide-Web:

http://www.cdt.org/

###

POLICY POST

September 11, 1995
Number 24

CENTER FOR DEMOCRACY AND TECHNOLOGY

A briefing on public policy issues affecting civil liberties online
---
CDT POLICY POST Number 24 September 11, 1995

CONTENTS: (1) Administration's New Crypto Policy Flops At Conference
(2) The Administration's Proposal
(2) Subcribe To The CDT Policy Post Distribution List
(3) About CDT, Contacting Us

---

(1) ADMINISTRATION CRYPTO POLICY FLOPS AT CONFERENCE

On September 6 and 7, the Clinton Administration unveiled a new national cryptography policy at a conference sponsored by the National Institute of Standards and Technology (NIST).

CDT believes that the new proposal fails to provide adequate privacy protection, would effectively eliminate the domestic market for non-escrowed encryption applications, and is weighed too heavily toward the interests of the National Security Agency.

The administration has proposed to relax export controls on cryptographic applications (both software and hardware) with key lengths up to 64 bits provided that:

The keys required to decrypt a message or file are escrowed with an agent certified by the US government (including private entities)

The product does not decrypt messages or files encrypted with non-escrowed products or products whose escrow mechanisms have been altered or disabled.

As well as eight other criteria (the proposal is attached below).

NEW PROPOSAL FAILS TO ADHERE TO CRITERIA IN GORE LETTER TO CANTWELL.

In a July 1994 letter to then Representative Maria Cantwell, Vice President Gore announced that the Administration intended to re-examine its cryptography policy. The Gore letter, which was widely viewed as an abandonment of the Clipper Chip Government Key Escrow scheme, pledged to develop a policy framework that would promote the development of encryption systems that would meet the following criteria:

Implementation in hardware of Software
Public, Unclassified Algorithms
Voluntary
Forth Amendment privacy Safeguards
Statutory liability rules to protect users
Multiple Escrow Agents

On hearing that the Administration had set out to develop a new encryption policy based on the principles outlined in the Gore letter, the Center for Democracy and Technology was guardedly optimistic that a genuine policy breakthrough was possible. However, having had the opportunity to review the current proposal, every principle, except the first (software implementation) and second (public algorithms), outlined in the July 1994 letter is violated or, in one case, left in doubt, by the September 1995 policy statement.

The September 1995 policy statement diverges from the July 1994 letter in the following critical respects. In our view, these divergences represent fundamental defects in the proposed policy.

NOT VOLUNTARY: The current proposal effectively compels all domestic users to use key escrow systems if they ever intend to communicate internationally. Point 6 of the export criteria requires that an exportable system must not interoperate with any system that non-escrow systems. Thus, in order for a user in the United States to communicate with anyone who uses a United States-made system on the Internet but outside of the United States, the American user must employ a key escrow system. Domestic users are not legally compelled to use key escrow products, but the proposed policy forces, in practice, all but the most insular Internet user toward a key escrow system. Moreover, this proposal further illustrates that the Administration seeks to use export controls to push the domestic use of escrowed cryptography. A policy based on such compulsion can hardly be called voluntary.

INADEQUATE SECURITY: Point 1 precludes export of systems with key lengths beyond 64 bits. Though this key size is larger than what is currently exportable, it is a level of security already judged inadequate for some applications. Given the rate at which computing power increases, even a 64 bit key would be subject to attach before long. Ironically, even the Clipper Chip provided a stronger (80 bit) key length

The premise of the key escrow policy is to provide law enforcement and national security agencies a "front door" to be used to decrypt messages when the agency obtains proper legal authorization. Yet, the

architects of the current policy apparently are not willing to trust that key escrow systems will meet law enforcement needs inasmuch as the key length limit suggests that the Administration is intent on maintaining an extra-legal method of decrypting communications. The Gore letter contains no suggestion that key escrow systems would also be subject to key length limits but the Administration seems to have lost faith in its own proposal. Such a half-hearted effort cannot be the basis of a long-lasting policy.

NO PRIVACY PROTECTION FOR USERS OF ESCROWED SYSTEMS: The ten export principles make no mention of privacy safeguards which the Vice President previously recognized as necessary to safeguard individual privacy and Fourth Amendment principles. Any escrow policy must contain safeguards against abuse and statutory liability provisions for the operators of private escrow systems.

FAILS TO PROMOTE INTERNATIONAL INTEROPERABILITY: Points 6 and 10 of the export criteria raise grave doubts as to the likelihood that the current proposal will give rise to a secure global communications environment. Point 10 forces users in other countries (and their governments) to accept United States-based escrow of all keys until bilateral access agreements are entered into. Such tactics seem unlikely to produce satisfactory international agreements, and hold global communications security hostage to the completion of such agreements.

NSA/ADMINISTRATION SEEK TO RUSH IMPLEMENTATION OF NEW POLICY

The NIST Key escrow conference was billed as an opportunity to begin a dialogue between the administration and industry on the new cryptography policy. However, as the conference began it quickly became apparent that many of the critical policy issues, including the 64 bit key length, interoperability with non-escrow products, and some requirements for key escrow agents (including whether individuals, corporations, and foreign entities are eligible) have already been decided.

The Administrations attempt to rush many of the critical policy decisions drew sharp reaction from virtually all of the conference participants, including CDT, other public interest groups, and representatives from several major software and hardware manufacturers. Although the administration and NSA officials all indicated that they got the message, they still intend to publish a revised policy in the next 30 days for comment.

INDUSTRY BALKS

Industry reaction to the new policy proposal was, with a few limited exceptions, decidedly negative. Both during formal presentations and in small group sessions, representatives from several of the largest hardware manufacturers and software publishers questioned whether the market would support products designed to adhere to the administration's proposal, particularly in light of the 64 bit key length limit.

CDT believes that the administration must make every effort to accommodate the concerns of the public, civil liberties groups, software publishers, hardware manufacturers, users, and other interested parties before adopting any new national cryptography policy. The current proposal fails to address many of the critical concerns of public interest groups and industry, and should be abandoned.

NEXT STEPS

The administration intends to published a revised policy within the next 30 days (October 7). CDT will closely monitor this issue and will inform you as it develops.

PATHS TO RELEVANT DOCUMENTS:

More information, including CDT's testimony from the NIST conference, other conference documents, etc. can be found at CDT's Crypto Issues Page:

URL:http://www.cdt.org/crypto.html

---

(2) THE ADMINISTRATION'S NEW CRYPTOGRAPHY POLICY

9/1/95 Proposed Cryptography Policy for Software Key Escrow

Key Escrow Issues Meeting, September 6-7, 1995
Discussion Paper #3

Export Criteria Discussion Draft --
64-bit Software Key Escrow Encryption

As discussed at the SPA/AEA meeting on August 17, 1995, the Administration is willing to allow the export of software encryption provided that the products use algorithms with key space that does not exceed 64 bits and the key(s) required to decrypt messages/files are escrowed with approved escrow agents. On the same date, the September 6-7 key escrow issues meeting at NIST was also announced. The two principal topics at the meeting will be: discussion of issues of exportability of 64-bit software key escrow encryption and 2) desirable characteristics for key escrow agents.

In order to help make most productive use of the limited time available at the upcoming meeting and to better focus deliberation, the following criteria are being distributed for discussion purposes. Since it is important that final criteria be clear, straightforward, consistent, and implementable, please review these draft criteria and be prepared to discuss how they may be refined and made more specific.

--- Draft Export Criteria ---

for Software Key Escrow Encryption

Software key escrow encryption products meeting the following criteria will be granted special export licensing treatment similar to that afforded other mass-market software products with encryption.

1. The product will use an unclassified encryption algorithm (e.g., DES, RC4) with a key length not to exceed 64 bits.

2. The product shall be designed to prevent multiple encryption (e.g., triple-DES).

3. The key required to decrypt each message or file shall be accessible through a key escrow mechanism in the product, and such keys will be escrowed during manufacture in accordance with #10. If such keys are not escrowed during manufacture, the product shall be inoperable until the key is escrowed in accordance with #10.

4. The key escrow mechanism shall be designed to include with each encrypted message or file, in a format accessible by authorized entities, the identity of the key escrow agent(s), and information sufficient for the escrow agent(s) to identify the key or key components required to decrypt that message.

5. The product shall be resistant to any alteration that would disable or circumvent the key escrow mechanism, to include being designed so that the key escrow mechanism cannot be disabled by a static patch, (i.e., the replacement of a block of code by a modified block).

6. The product shall not decrypt messages or files encrypted by non-escrowed products, including products whose key escrow mechanisms have been altered or disabled.

7. The key escrow mechanism allows access to a user's encrypted information regardless of whether that user is the sender or the intended recipient of the encrypted information.

8. The key escrow mechanism shall not require repeated involvement by the escrow agents for the recovery of multiple decryption keys during the period of authorized access.

9. In the event any such product is or may be available in the United States, each production copy of the software shall either have a unique key required for decrypting messages or files that is escrowed in accordance with #10, or have the capability for its escrow mechanism to be rekeyed and any new key to be escrowed in accordance with #10.

10. The product shall accept escrow of its key(s) only with escrow agents certified by the U.S. Government or by foreign governments with which the U.S. Government has formal agreements consistent with U.S. law enforcement and national security requirements.

Note: Software products incorporating additional encryption methods other than key escrow encryption methods will be evaluated for export on the basis of each encryption method included, as is already the case with existing products. Accordingly, these criteria apply only to the key escrow encryption method incorporated by a software product, and not to other non-escrowed encryption methods it may incorporate. For instance, non-escrowed encryption using a key length of 40 bits or less will continue to be exportable under existing export regulations.

---

(3) HOW TO SUBSCRIBE TO THE CDT POLICY POST LIST

CDT Policy Posts, which is what you have just finished reading, are the regular news publication of the Center For Democracy and Technology. CDT Policy Posts are designed to keep you informed on developments in public policy issues affecting civil liberties online.

SUBSCRIPTION INFORMAITON

1. SUBSCRIBING TO THE LIST

To subscibe to the policy post distribution list, send mail to "Majordomo@cdt.org" with:

subscribe policy-posts

in the body of the message (leave the subject line blank)

2. UNSUBSCRIBING FROM THE LIST

If you ever want to remove yourself from this mailing list, you can send mail to "Majordomo@cdt.org" with the following command in the body of your email message:

unsubscribe policy-posts youremail@local.host (your name)

(leave the subject line blank)

---

(4) ABOUT THE CENTER FOR DEMOCRACY AND TECHNOLOGY/CONTACTING US

The Center for Democracy and Technology is a non-profit public interest organization. The Center's mission is to develop and advocate public

policies that advance constitutional civil liberties and democratic values in new computer and communications technologies.

Contacting us:

General information on CDT can be obtained by sending mail to info@cdt.org

World-Wide-Web:

http://www.cdt.org/

ftp:

ftp://ftp.cdt.org/pub/cdt/

snail mail:

Center For Democracy and Technology
1001 G Street, NW Suite 700 East
Washington, DC 20001
voice: +1.202.637.9800
fax: +1.202.637.0968
###

POLICY POST

October 6, 1995
Number 25

CENTER FOR DEMOCRACY AND TECHNOLOGY

A briefing on public policy issues affecting civil liberties online
---
CDT POLICY POST Number 25 October 6, 1995

CONTENTS: (1) House Committeee Approves National ID System, Fight Moves to House Floor
(2) Breakdown of Committee Vote
(3) Statement of Rep. Chabot
(4) Subscription Information/How to Contact CDT

HOUSE JUDICIARY COMMITTEE APPROVE NATIONAL ID SYSTEM AS PROVISION OF IMMIGRATION BILL -- PROVISION IS WATERED DOWN, FIGHT MOVES TO HOUSE FLOOR

On September 20, 1995 members of the U.S. House of Representatives agreed to create a National Identification system. By a margin of 2 votes, the House Judiciary Committee failed to remove a provision of the House Immigration bill establishing a national registry of Social Security Administration and Immigration and Naturalization Service data. The Committee instead agreed to limit the scope of the system and to require Congressional authorization before large scale implementation. Excerpts from the Committee debate and the vote breakdown are printed below.

The effort to remove the national identification system provision is being led by Representative Steve Chabot (R-OH). Chabot offered an amendment to strike Section IV of HR. 2202, the "Immigration in the National Interest Act" (sponsored by Rep. Lamar Smith, R-TX) which would establish a national computer registry by combining Social Security Administration and Immigration and Naturalization Service data.

The 'Employment Eligibility Mechanism' as the provision is called in the legislation, would be used to monitor and track all hiring decisions made by employers nationwide. As a result, the ability of every American to work would be conditioned on the accuracy of the information in this national data system.

Chabot's effort to remove the Employment Eligibility Mechanism was narrowly

defeated 15 - 17. The committee instead approved an amendment offered by Rep. Martin Hoke (R-OH) to limit the scope of the program and require additional congressional authorization before a nation-wide system could be created. Debate now moves to the floor of the House, where another attempt to remove the provision altogether is likely.

The 'Employment Eligibility Mechanism' has been vigorously opposed by a large and diverse coalition, including organization such as the ACLU, Citizens for a Sound Economy, the Center for Democracy and Technology, and individuals such as William Kristol (Project for the Republican Future), Jeff Eisenach (Progress and Freedom Foundation), and Jack Kemp (Empower America), among others (for more information, see CDT Policy Post No.15 URL:http://www.cdt.org/publications/pp150531.html).

Representative Chabot's amendment to remove the Employment Eligibility Mechanism provision had broad bi-partisan support and the support of civil liberties advocates, ethnic organizations, business leaders, and labor and religious organizations. Chabot, who referred to the Employment Eligibility Mechanism as "1-800-BIG-BROTHER, deserves credit for bringing this issue to the forefront of the debate. Chabot has indicated that he will continue to press for the removal of the provision as the bill moves to the House Floor.

Although the Committee did not remove the Employment Eligibility Mechanism provision, Rep. Hoke (R-OH) offered an amendment to limit the Employment Eligibility Mechanism to a pilot program which would be conducted in at least 5 of the 7 states with the largest number of unauthorized workers. Under the Hoke amendment, the pilot projects sunset on October 1, 1991, and the system may not be established in non pilot states without additional action by Congress. In addition, Rep. Becerra (D-CA) added language directing the Attorney General to include an analysis of the system's: 1) ease and reliability; 2) impact on job loss due to inaccurate or unavailable data; 3) effect on discrimination; 4) impact on privacy; and , 5) cost and administration to employers. Both the Becerra and Hoke amendments were approved by a voice vote.

CDT is pleased that the Committee moved to limit the scope of the Employment Eligibility Mechanism and that Congressional approval would be required to expand the program. However, CDT remains vigorously opposed to government efforts to establish large scale national computer registries to track and verify personal information about US Citizens. Such proposals clearly violate the privacy rights of Americans, and create the potential for large scale surveillance by law enforcement agencies and discrimination by employers. CDT will closely monitor the progress of this issue and will update you on its progress as the House moves forward.

For More Information Contact:
Deirdre Mulligan, Staff Council
deirdre@cdt.org

---

(2) Breakdown of the Judiciary Committee vote to remove the Employment Eligibility Mechanism (EEM) section form the House Immigration

legislation (HR 2202)

In Favor of Removing the EEM Opposed to Removing the EEM

Jim Sensenbrenner, Jr. (R-WI) Henry J. Hyde (R-IL)
Bob Inglis (R-SC) Carlos J. Moorhead (R-CA)
Steve Buyer (R-IN) Bill McCollum (R-FL)
Martin R. Hoke (R-OH) George W. Gekas (R-PA)
Fred Heineman (R-NC) Howard Coble (R-NC)
Steve Chabot (R-OH) Lamar Smith (R-TX)
Michael P. Flanagan (R-IL) Steven H. Schiff (R-NM)
John Conyers (D-MI) Bob Barr (R-GA)
Patricia Schroeder (D-CO) Barney Frank (D-MA)
Jack Reed (D-RI) Charles E. Schumer (D-NY)
Jerrold Nadler (D-NY) Howard L. Berman (D-CA)
Melvin L. Watt (D-NC) John Bryant (D-TX)
Xavier Becerra (D-CA) Robert W. Goodlatte (R-VA)
Jose E. Serrano (D-NY) Sonny Bono (R-CA)
Zoe Lofgren (D-CA) Ed Bryant (R-TX)
Elton Gallegly (R-CA)
Charles T. Canady (R-FL)
Absent
Rick Boucher (D-VA)
Robert C. Scott (D-VA)
Sheila Jackson Lee (D-TX)

---

(3) Excerpts from Rep. Chabot's (R-OH) statement in favor of his amendment:

The system has been referred to as dialing 1-800-BIG-BROTHER. It will be costly to operate; it won't work; and it will send exactly the wrong message as to whether the government is to be the master or the servant of the people. Our focus should be on illegal immigrants and the people who smuggle them in, not on innocent, law abiding American citizens.

Now, some people argue that we should oppose this system because it will lead inevitably to a national ID card. . . But I believe that this system is tremendously misguided even if one does not believe that it will evolve into a national ID. We should stop this habit of turning to the private sector and forcing small business to act more and more as an arm of the federal government. And we should get the federal government out of the face of innocent citizens.

Would this 1-800 number system even work? I suppose that depends in part on your assumptions about whether those bad employers who now rely on undocumented labor would even call the number in the first place. And it depends, of course, on your assumptions about the infallibility of government data and government employees. Is everyone's name in the system now? No. Would every keystroke entered into the computer be perfectly executed? Perhaps, but an error rate of only one percent would at the very least cause great heartache for about 650,000 Americans each year. And while we may believe that government is perfect

(I confess I don't), would the employer always record the correct verification number? Personally, I worry about getting those verification numbers wrong every time I order some ticket by telephone.

Would government be able to resist the temptation gradually to expand the uses of this new system once the set-up costs have been incurred? Will we use it to track people, or to store more and more information on them? The answer again depends on your view of government, informed perhaps by your view as to whether use of the social security numbers has up to now been limited to their initial function.

But let's just consider the system at hand. I just don't think I was sent here to establish this sort of bureaucracy. And I'm not surprised that the spectrum of people opposing these provisions is extremely broad and encompasses folks who are all over the lot on other immigration issues.

My amendment will strengthen the bill, Mr. Chairman, for I do not believe that this legislation will be able to carry the weight of 1-800-BIG-BROTHER when it comes to the floor. I urge adoption of the amendment.

---

(4) HOW TO SUBSCRIBE TO THE CDT POLICY POST LIST

CDT Policy Posts, which is what you have just finished reading, are the regular news publication of the Center For Democracy and Technology. CDT Policy Posts are designed to keep you informed on developments in public policy issues affecting civil liberties online.

SUBSCRIPTION INFORMAITON

1. SUBSCRIBING TO THE LIST

To subscibe to the policy post distribution list, send mail to "Majordomo@cdt.org" with:

subscribe policy-posts

in the body of the message (leave the subject line blank)

2. UNSUBSCRIBING FROM THE LIST

If you ever want to remove yourself from this mailing list,
you can send mail to "Majordomo@cdt.org" with the following command
in the body of your email message:

unsubscribe policy-posts youremail@local.host (your name)

(leave the subject line blank)

---

(5) ABOUT THE CENTER FOR DEMOCRACY AND TECHNOLOGY/CONTACTING US

The Center for Democracy and Technology is a non-profit public interest organization. The Center's mission is to develop and advocate public policies that advance constitutional civil liberties and democratic values in new computer and communications technologies.

Contacting us:

General information on CDT can be obtained by sending mail to info@cdt.org

World-Wide-Web:

http://www.cdt.org/

ftp:

ftp://ftp.cdt.org/pub/cdt/

snail mail:

Center For Democracy and Technology
1001 G Street, NW Suite 700 East
Washington, DC 20001
voice: +1.202.637.9800
fax: +1.202.637.0968

POLICY POST

October 20, 1995
Number 26

CENTER FOR DEMOCRACY AND TECHNOLOGY

A briefing on public policy issues affecting civil liberties online
---
CDT POLICY POST Number 26 October 20, 1995

CONTENTS: (1) FBI Announces Digital Telephony Surveillance Capacity Request
(2) Subcribe To The CDT Policy Post Distribution List
(3) About CDT, Contacting Us

---

(1) FBI NOTICE BEGINS DIGITAL TELEPHONY COMPLIANCE PROCESS -- PUBLIC ACCOUNTABILITY FOR FBI REQUEST ESSENTIAL

On Monday October 16 1995, the FBI published its initial request for surveillance capacity as required under Section 104 (a) of the Communications Assistance for Law Enforcement Act (PL 104-144, a.k.a. Digital Telephony). As required by law, the FBI will accept public comments on the proposed capacity requirements for 30 days (ending November 15, 1995). The notice, which includes instructions for submitting comments, is attached below.

CDT is in the process of examining the proposed notice, and will issue formal comments in the next several weeks. We are evaluating the notice with the following criteria in mind:

Has the FBI met all the public accountability and oversight criteria required by the statute?

What is the impact of the proposed notice on the privacy of individual telephone subscribers and the security of telecommunications networks?

Does the requested capacity accurately reflect the needs of law enforcement?

The capacity requests are based on an FBI survey of recent surveillance activity. Is the factual justification for the FBI request sufficiently detailed to facilitate a substantial public discussion about the reasonableness of the needs?

Does the FBI expect telecommunications carriers to comply with the capacity requests if Congress fails to appropriate funds for reimbursement?

CDT plans to meet with the FBI to discuss the proposed notice. CDT will also work both on our own and through the Digital Privacy and Security Working Group (DPSWG, a coalition of over 50 public interest groups, telecommunications carriers, manufacturers, trade associations, coordinated by CDT), and with members of Congress to ensure that the reporting requirements and public accountability provisions of the law are enforced and that law enforcement provides the necessary accounting of its capability requests.

CDT stands ready to intervene as necessary before Congress, the Federal Communications Commission, the telecommunications industry standards bodies charged with setting technical standards for implementing the requirements, and at other points necessary to ensure that privacy is protected and the public accountability provisions are strictly enforced. We will continue to update you on developments on this issue as they occur.

BACKGROUND -- PUBLIC OVERSIGHT REQUIREMENTS IN THE DIGITAL TELEPHONY LAW

The Communications Assistance for Law Enforcement Act (CALEA) requires telecommunications carriers to ensure that their systems contain sufficient capability and capacity to permit law enforcement to conduct authorized electronic surveillance. However, the requirements of the statute do not apply to the Internet, commercial online services (such as America Online, Prodigy, or Compuserve), or BBS's.

The statute also contains specific new statutory privacy protections for transactional records generated by online electronic communications services, greater protection for cordless telephones, and prohibitions on pen register authority to gather location information ('pen registers' are devices used to gather dialed numbers). Furthermore, the statute contains provisions which require public accountability and oversight over law enforcement surveillance capacity requests, telecommunications carrier liability, standards setting, and cost reimbursement.

Although law enforcement officials must still obtain a search warrant in order to conduct a wiretap, the statute granted law enforcement new authority to influence the design of telecommunications networks. This authority must be closely monitored through the law's public accountability and oversight provisions to ensure that law enforcement does not over-reach or abuse the powers granted under the statute.

The statute separates compliance into two categories:

CAPACITY (The subject of the current notice): The ability of a telecommunications network to accommodate a specified number of intercepts, pen register, and trap and trace devices; and

CAPABILITY: Functional requirements to ensure that a telecommunications

network can enable law enforcement to conduct electronic surveillance.

Below is a basic overview of the compliance processes for both the capacity and capability requirements of the Digital Telephony law, along with a description of the proposed notice. A more detailed explanation of the compliance process, as well as the privacy and public accountability provisions can be found on CDT's Digital Telephony Web Page (URL:http://www.cdt.org/digtel.html)

SURVEILLANCE CAPACITY REQUIREMENTS

Section 104 of CALEA requires telecommunications carriers to ensure that their systems posses sufficient capacity to accommodate a specified number of simultaneous intercepts, pen register, and trap and trace devices. As required by Section 104 (a)(1), the FBI, after consultation with state and local law enforcement officials and the telecommunications industry, has published an initial notice or capacity requirements. Section 104 (a)(1) requires that the FBI seek public comment and then publish in the federal register and provide to telecommunications carriers:

1. NOTICE OF ACTUAL CAPACITY: The actual number of simultaneousintercepts, pen registers, and trap and trace devices that will be necessary 4 years from the date of enactment (October 25, 1998) (Sec 104 (a)(1)(A); and

2. NOTICE OF MAXIMUM CAPACITY: The maximum capacity required to accommodate all intercepts, pen registers, and trap and trace devices that the Attorney General estimates government agencies will be authorized to conduct simultaneously after the date 4 years after enactment (Sec 104 (a)(1)(B)).

Carriers then have 180 days to identify which aspects of their networks are not compliant with the published capacity requirements. Section 104 (e) requires the government to reimburse telecommunications carriers for all reasonable costs associated with capacity upgrades. If the government fails to reimburse a carrier, that carrier will not have to modify any feature or service. This provision is intended to ensure that the government prioritizes capacity requests and does not demand unnecessary surveillance capability financed by hidden charges to subscribers.

PROPOSED CAPACITY REQUIREMENTS

Throughout the past year, the FBI, through its Telecommunications Industry Liaison Unit (TILU) developed a "baseline of electronic surveillance activity" by compiling information from telecommunications carriers, law enforcement, U.S. District Courts, State Attorney's General, and State District Attorneys.

From this information, the FBI derived the total simultaneous electronic surveillance activity by switch and geographic area. Future capacity needs were determined by considering the impact of demographics, market trends, and "other factors" [page 53645, see below] (Section 104 (a)(2) gives the

FBI broad latitude in determining the basis of capacity needs).

As described above, the capacity requests include both "actual capacity" (which must be in place within 4 years), and "maximum capacity" (which must be in place after 1998). The FBI has proposed to create three categories of capacity requirements based on the projected number of simultaneous surveillance orders in geographic areas. Requirements are based on what the FBI refers to as the "engineered capacity" of each switch, feature, or service in a specific geographic region [page 53646, see below].

Although we contacted several telecommunications carriers, CDT has not yet been able to determine precisely what "engineered capacity" corresponds to. According to the FBI notice, engineered capacity refers to the maximum number of subscribers that can be served by a particular equipment, facility, or service. For the purposes of the descriptions below, we assume that the average number of subscribers is equal to 100,000 for each facility, equipment, or service deployed on a telecommunications carrier's network. Of course, it could be far more or less depending on the actual definition of the term and the number of subscribers per equipment, facility, or service.

CATEGORY III -- Baseline Surveillance Capacity

According to the notice, all telecommunications carriers would be required to meet the Category III requirements. The FBI estimates that roughly 75% of the U.S. would be covered by this category [page 53646, see below].

ACTUAL CAPACITY: .05% of engineered capacity, or 50 simultaneous surveillance orders for each equipment, facility, or service serving 100,000 subscribers.

MAXIMUM CAPACITY: .25% of engineered capacity, or 250 simultaneous surveillance orders for each equipment, facility, or service serving 100,000 subscribers, by 1998.

CATEGORY II -- Areas With Moderate Surveillance Activity

Carriers in geographic areas which the FBI estimates require higher than average surveillance capacity, including large suburban areas and some urban areas will be required to meet Category II and Category I requirements. The FBI estimates that roughly 25% of the U.S. will be covered by Category II and Category I [page 53646, see below].

ACTUAL CAPACITY: .25% of engineered capacity, or 250 simultaneous surveillance orders for each equipment, facility, or service serving 100,000 subscribers.

MAXIMUM CAPACITY: .5% of engineered capacity, or 500 simultaneous surveillance orders for each equipment, facility, or service serving 100,000 subscribers, by 1998.

CATEGORY I -- Areas With Heavy Surveillance Activity

Large urban areas and other areas the FBI estimates require the greatest surveillance capacity would fall under Category I [page 53646, see below].

ACTUAL CAPACITY: .5% of engineered capacity, or 500 simultaneous surveillance orders for each equipment, facility, or service serving 100,000 subscribers.

MAXIMUM CAPACITY: 1% of engineered capacity, or 1000 simultaneous surveillance orders for each equipment, facility, or service serving 100,000 subscribers, by 1998.

SURVEILLANCE CAPABILITY REQUIREMENTS

In addition to specific capability requirements, the Digital Telephony statute requires telecommunications carriers to ensure that they possess sufficient capability to enable law enforcement, pursuant to proper legal authorization, to (Section 103):

1. expeditiously isolate and intercept all wire and electronic communications within a carrier's network;

2. expeditiously isolate and enable the government to access call identifying information;

3. deliver intercepted communications and call-identifying information to a location specified by the government (but only with the affirmative intervention of the telecommunications carrier). Remote monitoring is explicitly prohibited;

4. to meet these requirements in a way that protects the privacy and security of communications and call-identifying information not authorized to be intercepted.

PROCESS FOR DETERMINING AND MEETING CAPABILITY REQUIREMENTS

The process for determining and meeting capability requirements (outlined in Sections 103 and 107 of the statute) is separate and distinct from the process for determining capacity requirements.

The CALEA requires law enforcement determine the specific capabilities it needs, and consult with appropriate telecommunications trade associations, standards setting bodies, representatives of users of telecommunications equipment, and State utility commissioners in order to determine what specific changes are required to meet the capability requirements (Sec 107 (a)).

The telecommunications industry, through standards-setting bodies, is charged with developing technical standards to meet the capability requirements (the statute explicitly prohibits the government from imposing any technical standards on the telecommunications industry). Finally, the standards can be challenged before the FCC if any person believes they do

not adequately protect privacy or fail to meet other requirements (Sec. 107 (e)). Carriers are responsible for meeting the capability requirements by October 1998.

The FBI is currently in the process of determining its specific capability needs

---

NEXT STEPS

When Congress passed the Digital Telephony bill last year, it simultaneously authorized, but did not appropriate, $500 million to reimburse telecommunications carriers capacity upgrades and capability upgrades where compliance is not 'reasonably achievable (Sec 109 (b)). If Congress fails to appropriate funds to cover reimbursement, telecommunications carriers will not be obligated to comply with the requirements of the statute.

The Administration has requested to fund the program through a 30-percent surcharge on civil monetary penalties and criminal fines at a level of $100 million dollars for fiscal year 1996. The request is currently part of the stalled anti-terrorism legislation. However, the FBI expects that funds will be appropriated as part of the Commerce, Justice, State appropriations bill, which is currently pending before the Congress.

CDT believes that no funds should be appropriated or spent to fund the implementation of the Digital Telephony law unless and until law enforcement demonstrates it has met the public accountability and oversight provisions. CDT is committed to working with the telecommunications industry, Congress, and the FBI to ensure that this requirement is met.

For More Information Contact:

Daniel Weitzner, Deputy Director: djw@cdt.org
Jonah Seiger, Policy Analyst: jseiger@cdt.org
---

(2) THE PROPOSED NOTICE OF CAPACITY REQUIREMENTS FROM THE FEDERAL REGISTER, OCTOBER 16 1995.

Note: Follow this link to view the text of the FBI's notice

---
(3) HOW TO SUBSCRIBE TO THE CDT POLICY POST LIST

To subscibe to the policy post distribution list, send mail to "Majordomo@cdt.org" with:

subscribe policy-posts

in the body of the message (leave the subject line blank)

---
(4) ABOUT THE CENTER FOR DEMOCRACY AND TECHNOLOGY/CONTACTING US

The Center for Democracy and Technology is a non-profit public interest organization based in Washington, DC. The Center's mission is to develop and advocate public policies that advance constitutional civil liberties and democratic values in new computer and communications technologies.

Contacting us:

General information: info@cdt.org
World Wide Web: URL:http://www.cdt.org
FTP URL:ftp://ftp.cdt.org/pub/cdt/

Snail Mail: The Center for Democracy and Technology
1001 G Street NW Suite 500 East Washington, DC 20001
(v) +1.202.637.9800 (f) +1.202.637.0968

End Policy Post No. 26

POLICY POST

October 24, 1995
Number 27

CENTER FOR DEMOCRACY AND TECHNOLOGY

A briefing on public policy issues affecting civil liberties online
---
CDT POLICY POST Number 27 October 24, 1995

CONTENTS: (1) Landmark Privacy Legislation Introduced in Senate -- Would Ensure Confidentiality of Medical Records
(2) CDT Led Coalition Letter In Support of Bennett Bill
(4) How To Subscribe To The CDT Policy Post Distribution List
(3) About CDT, Contacting Us

---

(1) LANDMARK PRIVACY LEGISLATION INTRODUCED IN SENATE

Bill Would Ensure Confidentiality of Medical Records

Landmark privacy legislation designed to protect the confidentiality of medical records was introduced today in the Senate by Senators Robert Bennett (R-UT), Robert Dole (R-KS), Nancy Kassebaum (R-KS), Edward Kennedy (D-MA), and Patrick Leahy (D-VT). If enacted, the "Medical Records Confidentiality Act" would create strong, comprehensive, privacy safeguards for the health data of all Americans. Similar legislation has been introduced in the House by Representative Gary Condit (D-CA).

As CDT Deputy Director Janlori Goldman stated during a press conference announcing the Introduction of the bill, "the Medical Records Confidentiality Act is desperately needed to close a gaping hole in current law that leaves peoples' most personal, sensitive information extremely vulnerable to abuse and misuse. Strong protections are needed to safeguard peoples' health records as the information moves on the Global information highway. Congress must seize the opportunity to pass this bill this session." Towards this end, CDT has organized a broad range of privacy and consumer advocates, along with representatives from the health care and information industries to work towards its passage. (see attached letter below)

The 'Medical Records Confidentiality Act' would:

Give people the right to see, copy, and correct their own medical records;

Limit disclosure of personal health information by requiring an individual's permission prior to disclosure of his or her health information by doctors, insurance companies, and other health information 'trustees' (e.g.: researchers and public heath departments);

Require the development of security guidelines for the use and disclosure of personal health information; and

Impose strict civil penalties and criminal sanctions for violations of the Act, and provide individuals with a private right of action against those who mishandle their personal medical information.

CDT believes that strong uniform privacy rules for the handling of personal health data are critical to ensuring public trust and confidence in the emerging health information infrastructure. Recent studies by the Institute of Medicine and the Office of Technology Assessment have shown that state laws are inadequate to protect peoples' health records, and that a federal law is needed to address this shortfall.

More information, including the text of the bill and a section-by-section summary, are available from CDT's Health Information Privacy web page (URL:http://www.cdt.org/health_priv.html).

BACKGROUND -- THE NEED FOR MEDICAL RECORDS PRIVACY PROTECTIONS

The public is continually told that increased data collection, linkage and sharing is necessary to improve the quality of health care and reduce costs. Yet without giving individuals confidence that their most sensitive personal information will be protected, we risk falling short of these health reform goals. If people don't trust the health care system to maintain the confidentiality of personal health information, they will be reluctant to fully participate. A 1993 Lou Harris poll shows that a majority of Americans favors new, comprehensive legislation to protect the privacy of medical records. The poll found that nearly 50 million people believe their own medical records have been improperly disclosed.

It is no wonder individuals are nervous about the privacy of their health information. One need only read the paper to learn about leaks of the sensitive health information of politicians, sports figures, and celebrities. The ordeals of Representative Nydia Velazquez (D-NY) and the late tennis star Arthur Ashe expose the dire consequences that can occur when health information is wrongly disclosed. Both Velazquez and Ashe suffered the disclosure of the most private intimate details of their lives -- a suicide attempt and HIV infection respectively -- to the world.

Public figures are not the only victims of unauthorized, egregious

disclosures. The average American also suffers from leaks of sensitive medical information. Recently, information on the HIV status, drug-abuse history, and sexual practices of volunteers at an Ohio Health Department's AIDS prevention unit was wrongly disclosed. Following another breach of confidential information, the office closed for retraining.

Weak security also leads to unauthorized internal access and misuse of peoples' health records. In March of this year, a 13-year-old daughter of a hospital clerk printed out the names and phone numbers of patients who had been treated at the University of Florida's Medical Center. As a hoax, the 13-year old girl then contacted seven patients and erroneously told them they were infected with HIV. After receiving one of these prank calls, a young girl attempted suicide believing she had the HIV virus.

CDT believes that the Medical Records privacy act is the most important privacy bill since the Electronic Communications Privacy Act of 1986 (ECPA). Furthermore, enacting health information privacy legislation is a critical first step in health care reform. The Medical Records Confidentiality Act is supported by nearly everyone with a stake in the debate. If passed, CDT believes the legislation will go a long way to restore the public's faith and confidence in the integrity and security of our nation's health care system.

NEXT STEPS:

The bill has been referred to the Senate Labor and Human Resources Committee (Chaired by Sen. Kassebaum (R-KS), a co-sponsor). Committee hearings are scheduled for mid-November, and the bill is expected to be considered by the full Senate early in 1996. Similar legislation is pending in the House (HR 435, sponsored by Rep. Condit (D-CA).

---

(2) CDT LED COALITION LETTER IN SUPPORT OF BENNETT BILL

October 20, 1995

Senator Robert Bennett
431 Dirksen Senate Office Bldg
Washington, DC 20510

Dear Senator Bennett:

We write to express our appreciation and strong support for your efforts to enact a comprehensive privacy law to protect personal health information. We believe that safeguarding the privacy of peoples' health information is a necessary and critical component of health care reform. As the health system's infrastructure grows increasingly automated, it is essential that people have confidence that their participation in the health care system does not mean the loss of their privacy.

Although we are still in the process of resolving certain issues in the draft Medical Records Confidentiality Act developed by your office, a substantial consensus has emerged on the central policy of providing Americans uniform, strong confidentiality protection for their health information.

We look forward to continuing to work with you on this important bill.

Sincerely,

Aimee Berenson
AIDS Action Council

Kathleen Frawley
American Health Information Management Association

Rick Pollack
American Hospital Association

American Association of Retired Persons

Leanord Rubenstein
Bazelon Center for Mental Health Law

Joel Gimpel
Blue Cross and Blue Shield Association

Janlori Goldman
Center for Democracy and Technology

Arthur Levin
Center for Medical Consumers

Christopher G. Caine
IBM Corporation

Susan Jacobs
Legal Action Center

John Rector
National Association of Retail Druggists

Blair Horner
New York Public Interest Group

Don E. Detmer, M.D.
University of Virginia Health Sciences Center

---
(3) HOW TO SUBSCRIBE TO THE CDT POLICY POST LIST

CDT Policy Posts, which is what you have just finished reading, are the

regular news publication of the Center For Democracy and Technology. CDT Policy Posts are designed to keep you informed on developments in public policy issues affecting civil liberties online.

SUBSCRIPTION INFORMAITON

1. SUBSCRIBING TO THE LIST

To subscibe to the policy post distribution list, send mail to "Majordomo@cdt.org" with:

subscribe policy-posts

in the body of the message (leave the subject line blank)

2. UNSUBSCRIBING FROM THE LIST

If you ever want to remove yourself from this mailing list, you can send mail to "Majordomo@cdt.org" with the following command in the body of your email message:

unsubscribe policy-posts youremail@local.host (your name)

(leave the subject line blank)

You can also visit our subscription web page URL:http://www.cdt.org/join.html

---

(4) ABOUT THE CENTER FOR DEMOCRACY AND TECHNOLOGY/CONTACTING US

The Center for Democracy and Technology is a non-profit public interest organization based in Washington, DC. The Center's mission is to develop and advocate public policies that advance constitutional civil liberties and democratic values in new computer and communications technologies.

Contacting us:

General information: info@cdt.org
World Wide Web: URL:http://www.cdt.org
FTP URL:ftp://ftp.cdt.org/pub/cdt/

Snail Mail: The Center for Democracy and Technology
1001 G Street NW Suite 500 East Washington, DC 20001
(v) +1.202.637.9800 (f) +1.202.637.0968

End Policy Post No. 27

POLICY POST

November 6, 1995
Number 28

CENTER FOR DEMOCRACY AND TECHNOLOGY

A briefing on public policy issues affecting civil liberties online
---
CDT POLICY POST Number 28 November 6, 1995

CONTENTS: (1) Senator Leahy Calls on FBI to Justify Surveillance Capacity
Request
(2) Text of Senator Leahy's Letter to FBI Director Freeh
(3) Review of Digital Telephony Implementation to Date
(4) How To Subscribe To The CDT Policy Post Distribution List
(5) About CDT, Contacting Us

-

(1) SENATOR LEAHY CALLS ON FBI TO JUSTIFY SURVEILLANCE CAPACITY REQUESTS

FBI Must Disclose Data to Ensure Public Accountability

US Senator Patrick Leahy (D-VT) on Friday November 3rd called on the FBI to disclose critical information justifying the its recent request for wiretapping capacity under the Communications Assistance for Law Enforcement Act (CALEA, a.k.a. the "Digital Telephony" law).

CDT commends Senator Leahy for his leadership on this issue and his efforts to ensure a detailed public discussion of the necessity of the FBI's request. CDT believes that Congress should not appropriate any funds to cover the costs of capacity modifications until the FBI justifies its need for the proposed surveillance capacity.

The FBI's proposal, published in the October 16 Federal Register, has sparked a great deal of concern from privacy advocates and the telecommunications industry that the FBI is seeking to expand its ability to wiretap digital telecommunications networks beyond its current activity the analog environment. In response to this concern, Senator Leahy sent the attached letter to FBI Director Freeh calling on the FBI to disclose two critical pieces of information used by the Bureau to determine its capacity needs: a survey of historical

surveillance activity and an analysis of that activity. The FBI's announcement of the proposed surveillance capacity did not contain this information.

Under CALEA, the FBI is required to publish requests for surveillance capacity in order to ensure public oversight and accountability over law enforcement surveillance activity. In addition, CALEA requires that the government reimburse telecommunications carriers for any modifications made to meet the capacity requests. If the government fails to reimburse telecommunications carriers for capacity modifications, carriers are not required to make any changes to their networks. Congress is currently considering legislation to appropriate funding for the proposal.

These provisions of CALEA were specifically designed to ensure a public debate over the necessity and costs of law enforcement surveillance capacity.

CDT will continue to work closely with Senator Leahy, other members of Congress, and representatives from the public interest community and the telecommunications industry to ensure that the public accountability provisions of the law are followed, and that Congress carefully examines the basis of the FBI's request before approving funding for the proposal.

---

(2) LETTER FROM SENATOR LEAHY TO FBI DIRECTOR FREEH

November 3, 1995

The Honorable Louis J. Freeh
Federal Bureau of Investigation
J. Edgar Hoover Building
9th Street and Pennsylvania Avenue
Washington, D.C. 20035

Dear Director Freeh:

Congress took the important step in the last Congress of passing the "Communications Assistance for Law Enforcement Act" (CALEA) to ensure that in cases of significant criminal activity, ranging from terrorism to kidnapping, law enforcement would continue to be able to execute court-authorized electronic surveillance. Our Nation's law enforcement agencies are loosing their capability to use that important tool in the face of new and advanced telecommunications technologies.

Just as significantly, this new law also brings decisions affecting the privacy of our Nation's telephone system under statutory guidance and into the sunshine. CALEA requires that law enforcement's demands regarding the number of wiretap orders that telephone companies must be able to service simultaneously, are published in the Federal Register and scrutinized in a public procedure.

The process set up in CALEA is working. The Federal Bureau of Investigation recently published in the Federal Register a proposed notice of law enforcement's capacity demands predicated upon an historical baseline of electronic surveillance activity and an analysis of that activity. The Federal Register notice did not include publication of those two documents.

Please provide me with copies of those two documents, which I also urge you to release to the public and publish in the Federal Register to ensure the fullest dissemination of the information.

I appreciate your prompt attention to this matter.

Sincerely,

[signature]
PATRICK J. LEAHY
United States Senator

---

(3) REVIEW OF DIGITAL TELEPHONY PROCESS TO DATE

FBI Must Address Critical Questions About The Proposed Capacity Notice

On October 16, 1995, the FBI published in the Federal Register its proposed notice of surveillance capacity, as required by CALEA. The FBI has requested that telecommunications carriers, depending on the geographic area served by their network and the frequency of surveillance orders in those areas, reserve up to 1% of the capacity of each switch, feature, or service for law enforcement to conduct simultaneous electronic surveillance pursuant to proper legal authorization.

CDT hopes that the publication of the basis of the FBI's surveillance capacity request will help to answer several critical questions about the proposal. These include:

ARE THE PROPOSED SURVEILLANCE CAPACITY REQUIREMENTS CONSISTENT WITH LAW ENFORCEMENT'S REAL NEEDS?

Is the FBI seeking to expand its surveillance capacity in digital telecommunications networks beyond its current activity in the analog environment?

The FBI has requested that, at a minimum, all telecommunications carriers nationwide ensure that .05% (.25% after 1998) of the "engineered capacity" of their networks be reserved for simultaneous surveillance activity, including wiretaps, trap and trace, and pen-registers (devices used to capture dialed number information). Greater capacity would be required in some areas (up to 1% by 1998 in the most populated parts of the US).

Although there is some dispute about what is meant by the term "engineered capacity", the proposed notice appears to allow law enforcement the ability to conduct a great deal more surveillance activity than they currently undertake (estimated to be between 850 and 1,000 per year nationwide).

WHAT ARE THE REAL NUMBERS?

How much capacity is being asked for and how does it compare with today's surveillance levels?

The proposed surveillance capacity requirements are based on a percentage of the "engineered capacity" of the telecommunications network. In the notice, the FBI defines "engineered capacity" as "the maximum number of subscribers that can be served by that equipment, facility, or service". There is some dispute over the meaning of this term.

Taken on its face, the FBI's definition of "engineered capacity" appears to grant the FBI the capacity to conduct up to 1 wiretap for every 100 telephone subscribers in densely populated areas. The FBI disputes this number, and has stated that "engineered capacity" refers to the number of subscribers who can be serviced simultaneously by a particular facility, equipment, or service. The FBI maintains that by this definition, the actual number of simultaneous wiretaps would be far lower than some have estimated.

Making public the basis of the FBI's surveillance capacity requests will help to clarify this issue. However, regardless of the actual number, the FBI must demonstrate that it is not requesting unnecessary surveillance capacity.

DIRECT NEGOTIATIONS WITH TELECOMMUNICATIONS CARRIERS FOR SURVEILLANCE CAPACITY ABOVE THE NATIONAL MINIMUM?

The FBI has proposed to undertake direct negotiations with telecommunications carriers for surveillance capacity beyond the proposed national minimum standard requested in the notice.

When Congress passed CALEA last year, it created a public process to bring law enforcement's electronic surveillance ability under public scrutiny in order to balance the new authority to influence the design of telecommunications networks.

The public accountability provisions of CALEA require the FBI to publish all surveillance capacity requests. Congress must take a critical look at this aspect of the FBI's proposal, and should not appropriate funds until the FBI agrees to disclose all capacity requests, as required by the law.

NEXT STEPS

Public Accountability Requirements Of The Statute Must Be Met

CDT will work closely with Senator Leahy and others to ensure that the FBI discloses the basis for its recent surveillance capacity request. Once the information is made available, we will work with Senator Leahy, other interested members of Congress, public interest groups and the telecommunications industry to ensure that the FBI does not receive unnecessary surveillance capacity. We will also work to ensure that no funding is made available until the public accountability provisions of the law are satisfied.

FOR MORE INFORMATION:

Visit CDT's Digital Telephony Web Page

http://www.cdt.org/digtel.html

---

(4) HOW TO SUBSCRIBE TO THE CDT POLICY POST LIST

CDT Policy Posts, which is what you have just finished reading, are the regular news publication of the Center For Democracy and Technology. CDT Policy Posts are designed to keep you informed on developments in public policy issues affecting civil liberties online.

SUBSCRIPTION INFORMAITON

1. SUBSCRIBING TO THE LIST

To subscibe to the policy post distribution list, send mail to "Majordomo@cdt.org" with:

subscribe policy-posts

in the body of the message (leave the subject line blank)

2. UNSUBSCRIBING FROM THE LIST

If you ever want to remove yourself from this mailing list, you can send mail to "Majordomo@cdt.org" with the following command in the body of your email message:

unsubscribe policy-posts youremail@local.host (your name)

(leave the subject line blank)

You can also visit our subscription web page URL:http://www.cdt.org/join.html

---

(5) ABOUT THE CENTER FOR DEMOCRACY AND TECHNOLOGY/CONTACTING US

The Center for Democracy and Technology is a non-profit public interest

organization based in Washington, DC. The Center's mission is to develop and advocate public policies that advance constitutional civil liberties and democratic values in new computer and communications technologies.

Contacting us:

General information: info@cdt.org
World Wide Web: http://www.cdt.org
FTP ftp://ftp.cdt.org/pub/cdt/

Snail Mail: The Center for Democracy and Technology
1001 G Street NW Suite 500 East Washington, DC 20001
(v) +1.202.637.9800 (f) +1.202.637.0968

End Policy Post No. 28 11/6/95

POLICY POST

November 9, 1995
Number 29

CENTER FOR DEMOCRACY AND TECHNOLOGY

A briefing on public policy issues affecting civil liberties online
---
CDT POLICY POST Number 29 November 9, 1995

CONTENTS: (1) Public Interest/Industry Coalition Says Administration Crypto
Policy Flawed -- Pledges to Develop Alternative
(2) Text of CDT-led coalition letter to Vice President Gore
(3) How To Subscribe To The CDT Policy Post Distribution List
(4) About CDT, Contacting Us

---

(1) Public Interest/Industry Coalition Says Administration Crypto Policy Flawed -- Pledges to Develop Alternative

A broad coalition of nearly forty public-interest organizations, trade associations, and representatives from the telecommunications and computer hardware and software industries sent the attached letter to Vice President Albert Gore on Wednesday, objecting to the Administration's recently announced cryptography policy.

While the letter praised the administration for its efforts to develop a national cryptography policy, the signatories, which include groups such as EFF and companies such as America Online, Apple, AT&T, MCI, Lotus, Microsoft, and Tandem Computer (organized by CDT), expressed concern that the Administration's proposal is weighed heavily in favor of law enforcement and national security while neglecting the privacy and security needs of individuals and the marketplace.

The letter states:

"A secure, private, and trusted Global Information Infrastructure (GII) is essential to promote economic growth and meet the needs of the Information Age society. Competitive businesses need cryptography to protect proprietary information as it flows across increasingly vulnerable global networks. Individuals require privacy protection in order to build the confidence necessary to use the GII for personal

and
financial transactions... The undersigned groups recognize that
the Administration's recently articulated cryptography initiative was
a
serious attempt to meet some of these challenges, but the proposed
initiative is no substitute for a comprehensive national cryptography
policy. To the extent that the current policy becomes a substitute
for
a more comprehensive policy, the initiative actually risks hindering
the development of a secure and trusted GII."

The coalition pledged to work together to formulate recommendations for
an alternative cryptography policy based on the following principals:

ROBUST SECURITY: access to levels of encryption sufficient to address
domestic and international security threats, especially as advances in
computing power make currently deployed cryptography systems less
secure.

INTERNATIONAL INTEROPERABILITY: the ability to securely interact
worldwide.

VOLUNTARY USE: freedom for users to choose encryption solutions,
developed in the marketplace, that meet their particular needs.

ACCEPTANCE BY THE MARKETPLACE: commercial viability and ability to
meet the expressed needs of cryptography users.

CONSTITUTIONAL PRIVACY PROTECTIONS: safeguards to ensure basic Fourth
Amendment privacy protection and regulation of searches, seizures, and
interceptions.

RESPECT FOR THE LEGITIMATE NEEDS OF LAW ENFORCEMENT and national
security, while recognizing the reality that determined criminals will
have access to virtually unbreakable encryption.

A second group, composed of conservative/libertarian organizations
including Americans for Tax Reform and Citizens for A Sound Economy,
issued a similar letter on Wednesday to House Speaker Newt Gingrich. The
text of that letter, as well as additional information on the
cryptography policy debate, can be found on CDT's Cryptography Issues
Page:

URL:http://www.cdt.org/crypto.html

The letters come as the National Institute of Standards & Technology
(NIST) this week announced revisions to the Administration's proposed
export criteria announced last September (See CDT Policy Post No. 24).
The revised proposal is substantively similar to the previous version,
and maintains controversial provisions including:

LIMITS ON KEY LENGTH: The revised proposal would continue to only
allow the export of cryptography systems with 64 bit key lengths, but

only if the keys are escrowed by an agent approved by the U.S. Government and if the systems meet the other export criteria.

RESTRICTED INTEROPERABILITY: While the revised proposal does clarify the interoperability provision, it would continue to prohibit exportable products from operating with any other cryptographic products that do not meet the NIST criteria.

NO PRIVACY SAFEGUARDS: The proposal contains no mention of the procedures for law enforcement access to escrowed keys, the standards for certifying escrow agents, or the obligations on escrow agents to protect privacy.

CDT believes that the NIST proposals fall far short of the promise for a more sensible and comprehensive cryptography policy outlined last July in Vice President Gore's letter to Rep. Maria Cantwell. The current proposal fails to provide adequate security, protect the privacy of individuals, and meet the needs of the global marketplace. CDT believes that a more comprehensive approach to cryptography policy is necessary to address both the immediate need for strong cryptographic applications and the long-term development of a secure and trusted Global Information Infrastructure. CDT will work with the signatories of the letter to over the next six months to develop an alternative to the Administration's proposal.

---

(2) Text of CDT-led Coalition Letter to Vice President Gore

November 8, 1995

The Honorable Albert Gore, Jr.
Office of the Vice President
Old Executive Office Building, Room 276
Washington, D.C. 20501

Dear Mr. Vice President:

A secure, private, and trusted Global Information Infrastructure (GII) is essential to promote economic growth and meet the needs of the Information Age society. Competitive businesses need cryptography to protect proprietary information as it flows across increasingly vulnerable global networks. Individuals require privacy protection in order to build the confidence necessary to use the GII for personal and financial transactions. Promoting the development of the GII and meeting the needs of the Information Age will require strong, flexible, widely-available cryptography. The undersigned groups recognize that the Administration's recently articulated cryptography initiative was a serious attempt to meet some of these challenges, but the proposed initiative is no substitute for a comprehensive national cryptography policy. To the extent that the current policy becomes a substitute for a more comprehensive policy, the initiative actually risks hindering the

development of a secure and trusted GII.

A number of the undersigned organizations have already written to express concern about the latest Administration cryptography initiative. As some of us have noted, the Administration's proposed export criteria will not allow users to choose the encryption systems that best suit their security requirements. Government ceilings on key lengths will not provide an adequate level of security for many applications, particularly as advances in computing render current cryptography systems less secure. Competitive international users are steadily adopting stronger foreign encryption in their products and will be unlikely to embrace U.S. restrictions. As they stand, current export restrictions place U.S. hardware manufacturers, software developers, and computer users at a competitive disadvantage, seriously hinder international interoperability, and threaten the strategically important U.S. communications and computer hardware and software industries. Moreover, the Administration policy does not spell out any of the privacy safeguards essential to protect individual liberties and to build the necessary public trust in the GII.

The current policy directive also does not address the need for immediate liberalization of current export restrictions. Such liberalization is vital to enable U.S. companies to export state-of-the-art software products during the potentially lengthy process of developing and adopting a comprehensive national cryptography policy. Without relief, industry and individuals alike are faced with an unworkable limit on the level of security available and remain hamstrung by restrictions that will not be viable in the domestic and international marketplace.

Many members of the undersigned groups have been working actively with the Administration on a variety of particular applications, products, and programs promoting information security. All of us are united, however, by the concern that the current network and information services environment is not as secure as it should be, and that the current policy direction will delay the secure, private, and trusted environment that is sought.

Despite the difficulties of balancing the competing interests involved, the undersigned companies, trade associations, and privacy organizations are commencing a process of collective fact-finding and policy deliberation, aimed at building consensus around a more comprehensive cryptography policy framework that meets the following criteria:

ROBUST SECURITY: access to levels of encryption sufficient to address domestic and international security threats, especially as advances in computing power make currently deployed cryptography systems less secure.

INTERNATIONAL INTEROPERABILITY: the ability to securely interact worldwide.

VOLUNTARY USE: freedom for users to choose encryption solutions,

developed in the marketplace, that meet their particular needs.

ACCEPTANCE BY THE MARKETPLACE: commercial viability and ability to meet the expressed needs of cryptography users.

CONSTITUTIONAL PRIVACY PROTECTIONS: safeguards to ensure basic Fourth Amendment privacy protection and regulation of searches, seizures, and interceptions.

RESPECT FOR THE LEGITIMATE NEEDS OF LAW ENFORCEMENT and national security, while recognizing the reality that determined criminals will have access to virtually unbreakable encryption.

In six months, we plan to present our initial report to the Administration, the Congress, and the public in the hopes that it will form the basis for a more comprehensive, long-term approach to cryptography on the GII. We look forward to working with the Administration on this matter.

Sincerely,

American Electronics Association
America Online, Inc.
Apple Computer, Inc.
AT&T
Business Software Alliance
Center for Democracy & Technology
Center for National Security Studies
Commercial Internet eXchange Association
CompuServe, Inc.
Computer & Communications Industry Association
Computing Technology Industry Association
Crest Industries, Inc.
Dun & Bradstreet
Eastman Kodak Company
Electronic Frontier Foundation
Electronic Messaging Association
EliaShim Microcomputers, Inc.
Formation, Inc.
Institute for Electrical and Electronic Engineers - United States Activities
Information Industry Association
Information Technology Industry Council
Information Technology Association of America
Lotus Development Corporation
MCI
Microsoft Corporation
Novell, Inc.
OKIDATA Corporation
Oracle Corporation
Securities Industry Association
Software Industry Council
Software Publishers Association

Software Security, Inc.
Summa Four, Inc.
Sybase, Inc.
Tandem Computers, Inc.
Telecommunications Industry Association
ViON Corporation

---

(3) HOW TO SUBSCRIBE TO THE CDT POLICY POST LIST

CDT Policy Posts, which is what you have just finished reading, are the regular news publication of the Center For Democracy and Technology. CDT Policy Posts are designed to keep you informed on developments in public policy issues affecting civil liberties online.

SUBSCRIPTION INFORMAITON

1. SUBSCRIBING TO THE LIST

To subscibe to the policy post distribution list, send mail to "Majordomo@cdt.org" with:

subscribe policy-posts

in the body of the message (leave the subject line blank)

2. UNSUBSCRIBING FROM THE LIST

If you ever want to remove yourself from this mailing list, you can send mail to "Majordomo@cdt.org" with the following command in the body of your email message:

unsubscribe policy-posts youremail@local.host (your name)

(leave the subject line blank)

You can also visit our subscription web page
URL:http://www.cdt.org/join.html

---
(4) ABOUT THE CENTER FOR DEMOCRACY AND TECHNOLOGY/CONTACTING US

The Center for Democracy and Technology is a non-profit public interest organization based in Washington, DC. The Center's mission is to develop and advocate public policies that advance constitutional civil liberties and democratic values in new computer and communications technologies.

Contacting us:

General information: info@cdt.org

World Wide Web: URL:http://www.cdt.org
FTP URL:ftp://ftp.cdt.org/pub/cdt/

Snail Mail: The Center for Democracy and Technology
1001 G Street NW Suite 500 East Washington, DC 20001
(v) +1.202.637.9800 (f) +1.202.637.0968

End Policy Post No. 29 11/9/95

POLICY POST

December 1, 1995
Number 30

A briefing on public policy issues affecting civil liberties online
---
CDT POLICY POST Number 30 December 1, 1995

CONTENTS: (1) UPDATE: Conferees Close To Decision on Cyberporn Issue
(2) How To Subscribe To The CDT Policy Post Distribution List
(3) About CDT, Contacting Us

---

(1) UPDATE: CONFEREES CLOSE TO DECISION ON CYBERPORN ISSUE

>From all accounts, the telecom conferees are beginning to focus on the net-censorship issue at the staff level, and a decision could be reached in the next two weeks.

CDT has learned that the conferees are looking at several different approaches to dealing with the issue, and at this point all but one (White) look pretty grim. These are:

(1) A MODIFIED EXON PROPOSAL: Includes the CDA, the House-passed manager's amendments which prohibit sending indecent material online, and the Cox/Wyden bill.

(2) THE HYDE/CHRISTIAN COALITION PROPOSAL: Rep. Hyde has endorsed a proposal offered by conservative religious groups in October (the so-called Reed, Schafly, Meese proposal, circulated on the net a few weeks ago). This proposal is more restrictive than the Exon proposal

(3) THE GRASSLEY PROPOSAL: Conceptually similar to S. 892, the Grassley/Dole 'Protection of Children from Computer Pornography Act'. Among other things, the bill would create broad liability for online indecency for both content providers and online service providers, without any clear limitation.

(4) COX/WYDEN/WHITE: Rep. Rick White (R-WA), an original co-sponsor of Cox/Wyden, is preparing an alternative to the 3 proposals above. No word yet on what it will contain, although it is expected to focus

on parental empowerment as opposed to unconstitutional indecency restrictions and government regulation of online speech.

Unfortunately, none of the three current proposals on the table (EXON, HYDE, and GRASSLEY), offer much hope. The fourth, WHITE, does not yet exist, though the reports we have received indicate that it is likely to be more reasonable and workable than the others.

Below is an overview of the current status of the issue and an analysis of the three current proposals.

CURRENT STATUS OF CONFERENCE

A House/Senate conference committee is now in the process of reconciling the differences between the Senate-passed Exon/Coats CDA and the House-passed Cox/Wyden bill. Unfortuately, and despite the overwhelming victory of Cox/Wyden, the reports indicate that the CDA is sill very much alive.

Because the Senate passed the CDA, and because Exon is a member of the conference committee, Exon has the necessary leverage and support to push for his proposal. The same holds true on the House side, where the principal supporter of the Cox/Wyden position is Rep. Rick White. Ultimately, the conferees will have to decide how much of each proposal to accept.

The situation is complicated by the introcution of two new, even more restrictive proposals (Hyde and Grassley). These proposals have the support of the Christian Coalition (an influential group with many Republicans on the conference), meaning that we face a steep, uphill battle in the next few weeks.

OVERVIEW OF EXON, HYDE, AND GRASSLEY PROPOSALS

Below is an overview of how the 3 proposals treat several of the key issues, including the use of the indecency standard, the 'display' of indecent material online, FCC oversight of cyberspace, vicarious liability for service providers, preemption of inconsistent state laws, and defenses for service providers.

I. INDECENCY

All three seeks to prohibit indecent material on the Internet or other interactive media. As mentioned above, indecency is a broad classification of material including sexually explicit material, the '7 dirty words', and even classic works of fiction such as The Catcher In the Rye or Ulysses. As we have long argued, indecency restrictions on the Internet are unconstitutional given the tremendous amounts of control users have over the material they receive.

EXON: Prohibits creating, transmitting, or making available any indecent material to anyone under 18 (Sec 402 (a) - (e)). Violators face $100,000 fines and up to 2 years in jail

HYDE: Criminalizes transmission or display of indecent material to anyone under 18 (amendment to 18 USC 1465). Creates $100,000 fines and 2 years in jail for anyone who makes or makes available any indecent material to a minor (Sec 402 (d)).

GRASSLEY: Punishes 'Content Providers" who knowingly make an indecent communication to anyone under 18 (Sec (3)).

Also punishes "Access Providers' who 'willfully' provide a minor with access to a computer communications facility on which indecent communications are available (Sec. (f)).

Violators face $100,000 fines and up to 2 years in jail

II. 'DISPLAY CRIME'

All three proposals seek to prohibit the 'display' of indecent material in various ways. They are modeled on the concept of 'brown paper bags' or other blinders which cover adult magazines at 7-11 type stores, though in the online context the current proposals are much more restrictive and would apply to individual content providers (not just the owner of the store).

These provisions would apply to web pages, ftp and gopher archives, usenet newsgroups, etc.

EXON: Prohibits the display of indecent material to minors (Sec (e)(1)). Violators face $100,000 fines and 2 years in jail.

HYDE: Prohibits the display of indecent material to minors (Sec 402 (d)). Violators face $100,000 fines and 2 years in jail. Proposal is identical to Exon described above.

GRASSLEY: Prohibits the display of indecent material to minors (Sec (e)), as well as knowingly allowing a minor access to a computer network on which indecent material is available (Sec (f)). Under this provision, anyone who allows a minor access to the Internet, including an online service provider or even the child's parent, could go to jail if they "know" indecent material is available and allow a minor acess.

III. FCC ROLE

Two of the new proposals would grant the FCC new authority to regulate cyberspace.

EXON: Grants the FCC jurisdiction over online speech and over

blocking and filtering technologies (Sec (f)(1) - (4).

HYDE: Grants the FCC broad authority over online speech and over blocking and filtering technologies (Sec (e)(1)).

GRASSLEY: No FCC role proposed.

IV. VICARIOUS LIABILITY FOR CARRIERS

All three proposals would hold carriers criminally liable merely for transmitting content created by others. Holding carriers liable for content on their networks would (1) force carriers to ensure that their networks are not being used to transmit prohibited material (creating a free speech and privacy nightmare), or (2) remove all incentives for those carriers who may wish to exercise limited editorial control over their networks to act responsibly.

EXON: Amends 18 USC 1465 to prohibit 'transmission' by computer of indecent material to minors. This provision could be read to apply to apply to service providers (Sec. 410).

HYDE: Similar to Exon proposal, amendments to 18 USC 1465 would prohibit 'transmission' by computer of indecent material to minors. This provision could be read to apply to service providers.

GRASSLEY: Would hold access providers liable for knowingly providing minors access to a computer service on which indecent material is available (sec (f)).

V. PREEMPTION

More and more states are attempting to pass their own net-censorship bills. Some are more restrictive than others. However, because interactive media is interstate and international, entire networks will be forced to adhere to the most restrictive standards unless Congress enacts a uniform national policy and pre-empts states from enforcing inconsistent or incompatible regulations.

The pre-emption provisions vary between the three proposals:

EXON: Pre-empts states from imposing liability on commercial entities, nonprofit libraries and schools. However, states could enact tougher restrictions on individual users, BBS's, non-profit organizations, and non-profit computer networks (freenets) (Sec. (g)

HYDE: Contains no pre-emption of state laws, allowing states to impose stricter regulations and even enact inconsistent laws.

GRASSLEY: Explicitly prohibits pre-emption. States would be free to enact any restrictions, even if they are more restrictive (Sec (l)).

VI. DEFENSES

All three proposals contain defenses designed to protect service providers from liability in certain circumstances. While we have long held the position that defenses are important (since holding service providers liable for their subscribers content creates huge problems for free speech and privacy), it is not clear that all these defenses will work as advertised.

EXON: (1) No control -- Providers cannot be held liable for providing access to material if the provider has no control over the material (Sec (f)(1)).

(2) FCC Determination Of Good Faith -- Providers cannot be held liable if they have taken good faith actions, as prescribed by the FCC, to restrict access to prohibited material (Sec. (f)(3)).

(3) Employers -- Employers will not be held liable for the actions of an employee's activities online (unless the conduct is part of their job or the employer authorizes it) (Sec (f)(2)).

HYDE: (1) FCC Determination Of Good Faith -- No liability if a person has complied with regulations designed to restrict access to indecent communications to those under 18 as enacted by the FCC, which is required to prepare final regulations 120 days after passage of the bill.

No other defenses are offered.

GRASSLEY: (1) Defense for Screening -- The proposal creates a defense to prosecution if a person has taken good faith efforts to restrict or prevent the transmission of or access to indecent materials (Sec. (g))

(2) Employers -- Employers will not be held liable for the actions of an employee's activities online (unless the conduct is part of their job or the employer authorizes it) (Sec. h)

SUMMARY

While this may all seem pretty bleak, all is not lost just yet. As mentioned earlier, Rep. Rick White (R-WA) is reportedly about to offer an alternative to the Exon/Hyde/Grassley proposals. The White proposal is expected to be based on the Cox/Wyden/White 'parental empowerment'

approach.

However, even if the White approach is, as expected, preferable to the 3 alternatives, the fact that Exon, Hyde, and Grassley are all pushing more restrictive proposals means that it is unlikely we will come out of this with everything we want. The Christian Coalition is too powerful, especially with the Chairman of the House Judiciary Committee on their side, to not have some influence on the final outcome of this debate.

We have a great deal of work ahead of us. Once the White proposal is available, we will be able to get a better sense of our chances for salvaging a palatable outcome. We will keep you informed of developments as they occur.

BACKGROUND

As you know, the House and Senate have passed two very different approaches to dealing with objectionable material online as part of a massive telecommunications reform bill.

In June, the Senate passed the Exon/Coats CDA, which would create a crime for transmitting or displaying indecent material online. "Indecent" material is a vague and constitutionally suspect classification of material which includes everything from sexually explicit material to the '7 dirty words', to the text of classic works of fiction such as Catcher in the Rye. In addition, the Exon/Coats CDA would grant the FCC broad authority to regulate online speech as well as the underlying technology of the Internet and other interactive media.

In August, the House passed the Cox/Wyden/White 'Internet Freedom and Family Empowerment Act'. Cox/Wyden/White would prohibit the FCC from imposing content or other regulations on the Internet or other interactive media, remove disincentives which prohibit online service providers from deploying blocking and filtering applications, and create a uniform national policy of user control, rather than government censorship, for addressing objectionable material online. However, the House also passed the so-called 'Managers Amendments', which would criminalize sending indecent material to a minors.

FOR ADDITIONAL INFORMATION:

The text of the Exon, Hyde, and Grassley proposals are available on CDT's net-censorship issues web page (URL below). Additional background information, including the texts of the Senate-passed Exon Bill, Cox/Wyden, the House-passed 'manager's amendments', and other relevant material is also available at the CDT net-censorship page:

URL: http://www.cdt.org/cda.html

For additional information contact:

The Center for Democracy and Technology +1.202.637.9800

Daniel Weitzner, Deputy Director <djw@cdt.org>
Jonah Seiger, Policy Analyst <jseiger@cdt.org>

---
(2) HOW TO SUBSCRIBE TO THE CDT POLICY POST LIST

CDT Policy Posts, which is what you have just finished reading, are the regular news publication of the Center For Democracy and Technology. CDT Policy Posts are designed to keep you informed on developments in public policy issues affecting civil liberties online.

SUBSCRIPTION INFORMAITON

1. SUBSCRIBING TO THE LIST

To subscibe to the policy post distribution list, send mail to "Majordomo@cdt.org" with:

subscribe policy-posts

in the body of the message (leave the subject line blank)

2. UNSUBSCRIBING FROM THE LIST

If you ever want to remove yourself from this mailing list, you can send mail to "Majordomo@cdt.org" with the following command in the body of your email message:

unsubscribe policy-posts youremail@local.host (your name)

(leave the subject line blank)

You can also visit our subscription web page URL:http://www.cdt.org/join.html

---
(3) ABOUT THE CENTER FOR DEMOCRACY AND TECHNOLOGY/CONTACTING US

The Center for Democracy and Technology is a non-profit public interest organization based in Washington, DC. The Center's mission is to develop and advocate public policies that advance constitutional civil liberties and democratic values in new computer and communications technologies.

Contacting us:

General information: info@cdt.org
World Wide Web: URL:http://www.cdt.org
FTP URL:ftp://ftp.cdt.org/pub/cdt/

Snail Mail: The Center for Democracy and Technology
1001 G Street NW Suite 500 East Washington, DC 20001

(v) +1.202.637.9800 (f) +1.202.637.0968

End Policy Post No. 30 12/1/95

POLICY POST

December 4, 1995
Number 31

A briefing on public policy issues affecting civil liberties online
---
CDT POLICY POST Number 31 December 4, 1995

CONTENTS: (1) House Conferees to Vote Wednesday on Fate of Net
(2) How To Subscribe To The CDT Policy Post Distribution List
(3) About CDT, Contacting Us

-

(1) HOUSE CONFEREES TO VOTE WEDNESDAY ON FATE OF THE NET

On Wednesday December 6, members of the House conference committee will vote on how to deal with the controversial "cyberporn" issue. The full House/Senate conference committee will consider the issue within the next two weeks.

After months of contentious debate, the conferees must now choose between two proposals: one proposal sponsored by Representative Henry Hyde (R-IL) and an alternative proposed by Rep. Rick White (R-WA). The Hyde proposal would severely restrict freedom of speech on the Internet, and grant the Federal Communications Commission new authority to regulate online content. The White proposal relies on parents, not federal bureaucrats, to determine what material is and is not appropriate for themselves and their children, though it also imposes new criminal penalties for individuals who transmit material that is "harmful to minors".

The outcome of this decision will have tremendous implications on the future of freedom of expression and the development of interactive media as a whole. If the Hyde proposal prevails, the Internet as we know it will never be the same.

CDT firmly believes that no new laws in this area are necessary. Current law is already working to punish online stalkers and prosecute the distribution of obscene material online. However, choosing nothing is not an option available to the Conference Committee. Given the options before the committee, CDT believes that the effort of Congressman White should be commended. He has tried to find a resolution to this issue

which preserves freedom of speech and relies on user empowerment over government control of online content. Rep. White's proposal represents the only option on the table which will not destroy the Internet and the future of interactive communications technologies. Although this is a difficult choice for the Net.Community, White must prevail at this stage.

The Hyde proposal, which is being pushed heavily by the Christian Coalition, would severely restrict freedom of speech and the democratic potential of the Internet and other interactive media. It fails to recognize the global, decentralized nature of interactive media and its tremendous ability for user control. The proposal would be wholly ineffective at accomplishing its stated objective of protecting children from objectionable material, while destroying the Internet in the process.

If the conferees choose Hyde's approach over White, the Federal Communications Commission will, for the first time ever, have the authority to regulate online content and the underlying technologies of the net itself. In addition, the First Amendment and the free flow of information online will be chilled by an overly broad "indecency" standard. Online service providers will be forced to monitor all traffic to ensure that no "indecent" material is transmitted (creating a nightmare for freedom of speech and privacy), or shut down some service all together for fear of expensive law suits or prison sentences. And although all these provisions can be challenged in court, recent history with the so-called "dial-a-porn" and indecency an cable channels (Alliance for Community Media vs. FCC) suggest that such challenges can take years to resolve, and even then with no guarantee of success.

Representative White's approach seeks to protect cyberspace from intrusion by the federal government, and to empower parents to make decisions about what is and is not appropriate for themselves and for their children. While the proposal does contain new criminal provisions, including restrictions on the display of material that is "harmful to minors", it also creates a defense to prosecution for those who take good faith, reasonable efforts to label content and enable others to block it using user control technologies.

The fate of the Net, and the future of freedom of speech and the democratic potential of interactive media, now rests in the hands of the conference committee members.

OVERVIEW OF THE HYDE AND WHITE PROPOSALS

I. THE HYDE PROPOSAL

Representative Hyde is pushing an unconstitutional and overly regulatory proposal which would criminalize the transmission and display of "indecent material" (a broad classification which includes everything from the so-called '7 dirty words' to classic works of fiction such as The Catcher In the Rye and Ulysses), hold carriers liable for material created by their subscribers, and grant the Federal Government broad new

authority over online content and the underlying technologies of the Internet. The Hyde proposal has been endorsed by the Christian Coalition and other members of the "religious-right".

Among other things, the Hyde proposal would:

1. Create $100,000 fines and 2 year jail terms for anyone who makes or makes available any indecent material to a minor (Sec 402 (d)).

2. Grant the FCC broad authority over on line speech and over online technology (Sec (e)(1))

3. Criminalize the transmission or display of indecent material to anyone under 18 years of age (Amendment to 18 USC 1465),

4. Not pre-empt state from passing even more restrictive, or even inconsistent, regulations.

See CDT Policy Post No. 30 (December 1, 1995) for a detailed description of the Hyde proposal. For more information, including the text of the Hyde proposal and other relevant documents, visit CDT's net-censorship issues page (http://www.cdt.org/cda.html)

II. THE WHITE PROPOSAL

The proposal offered by Representative White, an original co-sponsor of the Cox/Wyden/White "Internet Freedom and Family Empowerment" Amendment, is based on the user empowerment aspects of the original Cox/Wyden/White amendment.

The White proposal substitutes the narrower "harmful to minors" standard for "indecency", and prohibits the FCC from imposing content regulations on online speech and from meddling in the underlying technologies of the Internet. While the White proposal does prohibit the "display" of material that is harmful to minors online, it creates a defense for those who take good faith, reasonable steps, to labile content and enable users to block or objectionable material using user control technologies (such as SurfWatch, the Parental Control features of AOL or Prodigy, or the PICS standards being developed by MIT and the World Wide Web Consortium).

Briefly, the White proposal would:

1. Prohibit intentionally sending material that is harmful to minors directly to a to someone the sender knows is a minor,

2. Prohibit the display of material that is harmful to minors. However, content providers (including individual users) would be immune to prosecution if they have taken good faith, reasonable efforts to labile their content and enable it to be blocked or filtered by others
(The MIT/World Wide Web consortium's PICS would be one example),

3. Prohibit the FCC from regulating content on or the technologies of the Internet and other interactive media,

4. Pre-empt inconsistent state laws, although this provision would not apply to individuals, non-profit providers of interactive computer services (such as BBS's or freenets), or non-profit organizations.

5. Clarify the House-passed Cox/Wyden/White to ensure that it does inadvertently create loopholes in ECPA or other privacy laws,

6. Protect online service providers from vicarious liability for transmitting their subscribers messages or for merely providing access to the Internet.

III. BACKGROUND ON THE "HARMFUL TO MINORS" STANDARD

White's proposal would prohibit sending material that is "harmful to minors" directly to a minor, as well as prohibit the display of material that is "harmful to minors" unless good faith, reasonable steps to labile and enable others to block access to such material.

Harmful to minors is an intermediate standard between indecency and obscenity. It is essentially material that is obscene to a minor. It has been used in 48 state statutes and has been ruled constitutional by the Supreme Court. It is defined as follows:

"'harmful to minors' means any communications or material that is obscene or that:

(a) taken as a whole, and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;

(b) depicts, represents, or describes in a patently offensive way with respect to what is suitable for minors, ultimate sexual acts, normal or perverted, actual or simulated, sado-masochistic acts or abuse; or lewd exhibition of the genitals, pubic area, buttocks, or post-putertal female breasts; and

(c) taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.

Materials that would be acceptable under this standard include the text of Catcher in the Rye, Ulysses, the use of the "7 dirty words" in context, and works of art which contain nudity. These same materials would be prohibited under an "indecency" standard.

NEXT STEPS

Once the House conferees vote on Wednesday, the full House/Senate conference committee will consider the issue. If the House conferees accept the White proposal, there will be additional opportunities to clarify and strengthen the proposal. However, if Hyde prevails, the entire battle will be lost.

In addition to the "cyberporn issue", there are several other issues in the telecommunications bill which the conferees much resolve, including competition in the long distance market, cable rate regulation, and universal service, to name a few. The Republican leadership has reportedly instructed the conferees to finish all remaining issues this week and to have the final bill ready for the full House and Senate during the week of December 11. It is not clear whether this deadline can actually be met given the range of unresolved issues, but the House and Senate leadership appear committed to the timeline.

CDT will keep you informed of developments on this issue as they occur. We will also post the text of the White proposal on our net-censorship web page as soon as a final copy is available (we expect it to be posted by Tuesday afternoon 12/5).

For more information, visit CDT's net-censorship issues page:

http://www.cdt.org/cda.html

---
(2) HOW TO SUBSCRIBE TO THE CDT POLICY POST LIST

CDT Policy Posts, which is what you have just finished reading, are the regular news publication of the Center For Democracy and Technology. CDT Policy Posts are designed to keep you informed on developments in public policy issues affecting civil liberties online.

SUBSCRIPTION INFORMAITON

1. SUBSCRIBING TO THE LIST

To subscibe to the policy post distribution list, send mail to "Majordomo@cdt.org" with:

subscribe policy-posts

in the body of the message (leave the subject line blank)

2. UNSUBSCRIBING FROM THE LIST

If you ever want to remove yourself from this mailing list,
you can send mail to "Majordomo@cdt.org" with the following command in the body of your email message:

unsubscribe policy-posts youremail@local.host (your name)

(leave the subject line blank)

You can also visit our subscription web page
URL:http://www.cdt.org/join.html

---
(3) ABOUT THE CENTER FOR DEMOCRACY AND TECHNOLOGY/CONTACTING US

The Center for Democracy and Technology is a non-profit public interest organization based in Washington, DC. The Center's mission is to develop and advocate public policies that advance constitutional civil liberties and democratic values in new computer and communications technologies.

Contacting us:

General information: info@cdt.org
World Wide Web: URL:http://www.cdt.org
FTP URL:ftp://ftp.cdt.org/pub/cdt/

Snail Mail: The Center for Democracy and Technology
1001 G Street NW Suite 500 East Washington, DC 20001
(v) +1.202.637.9800 (f) +1.202.637.0968

End Policy Post No. 31 12/4/95

POLICY POST

December 6, 1995
Number 32

A briefing on public policy issues affecting civil liberties online
---
CDT POLICY POST Number 32 December 6, 1995

CONTENTS: (1) House Conferees Approve Sweeping Net-Censorship Proposal
White Proposal Approved, Then Gutted by Religious Conservatives
2 Liberal Democrats Abandon the First Amendment
Senate Passage Expected Without Substantial Amendment
Court Challenge Likely
(2) How To Subscribe To The CDT Policy Post Distribution List
(3) About CDT, Contacting Us

---

(1) HOUSE CONFEREES APPROVE SWEEPING NET-CENSORSHIP PROPOSAL

House Conferees Approve Sweeping Net-Censorship Proposal

By a razor thin margin, members of the House Conference Committee on Telecommunications Reform have approved a broad proposal to censor constitutionally protected speech on the Internet. The provisions adopted today would make the Internet and Interactive media the most heavily regulated communicatoins medium in the United States, and severely threaten the future of free expression and democratic values in the information age.

The proposal, if agreed to by the full conference committee, would impose $100,000 fines and prison terms for anyone who posts any "indecent" material, including the "7 dirty words", the text of classic works of fiction such as The Catcher In The Rye, or Ulysses, artwork containing images of nudes, rap lyrics, in a public forum.

CDT strongly opposes the legislation agreed to by the House conferees today. We believe this proposal threatens the very existence of the Internet as a means for free expression, education, and political discourse. The proposal is an unwarranted, unconstitutional intrusion by the Federal government into the private lives of all Americans.

Indecent material is constitutionally protected speech which the Supreme Court has ruled can only be restrictive through the "least restrictive

means". Material that has been considered "indecent" has included, among other things:

The so-called "7 dirty words"
The Catcher In The Rye
Sex and AIDS Education literature
Photographic, sculpted, and painted images of nudes
Rap Lyrics

Posting any of the above materials in a public forum would be illegal under the provision approved today. Although it is unrealistic to expect that Federal law enforcement has the resources to go after each and every violation, the threat of $100,000 fines and 2 year prison sentences will result in a severe chilling effect over all online communications.

CDT will devote all our efforts in the coming weeks to ensure that the full conference committee does not endorse the approach approved today by the House. We are also committed to fighting this battle all the way to the Supreme Court, if necessary, to ensure that these provisions are overturned.

The text of the proposal will be placed on CDT's net-censorship web page (URL below) as soon as it's available. CDT will also post a detailed analysis of the bill soon.

WHITE PROPOSAL ADOPTED, THEN AMENDED TO INCLUDE INDECENCY STANDARD
2 LIBERAL DEMOCRATS TIP THE SCALES IN FAVOR OF RELIGIOUS-RIGHT

At today's meeting of the House and Senate Conference Committee members, Rep. Henry Hyde (R-IL) offered his proposal to prohibit the transmission and display of indecent material online, and grant the FCC new authority to regulate the Internet. As expected, Rep. Rick White (R-WA) offered his alternative, based on the narrow and constitutional "harmful to minors" standard and provisions to encourage parental control, not government censorship. The House conferees then adjourned to a private room, away from the press and television cameras, to vote.

The Conferees voted 20 - 13 to accept the White proposal. However, Rep. Goodlatte (R-VA) offered an amendment to substitute "indecency" for the "harmful to minors" standard in the White proposal. The Goodlatte amendment was approved on a vote of 17 - 16 and the "harmful to minors" standard was replaced by the blatantly unconstitutional "indecency standard". Representative White did NOT vote for the Goodlatte amendment.

Amazingly, two traditionally liberal democrats, Reps. Pat Schroeder (D-CO) and John Conyers (D-MI) voted for the "indecency" standard! Had either of these members voted the other way, libraries, schools, and even parents who allow children to access the text of The Catcher In The Rye online would not now face $100,000 fines and prison sentences. Schroeder and Conyers should be ashamed of themselves for not standing up for freedom of speech and democratic values at such a critical moment, and for assisting the campaign of religious conservatives to impose their moral values on the Internet without regard for long-standing constitutional principals.

Representative White should be commended for his efforts to craft a constitutional proposal which preserved freedom of speech and relied on user empowerment over government control of online content. He deserves great credit for his commitment to protecting the Internet and preserving freedom of speech, and his willingness to stand up to religious conservatives. Unfortunately, the critical element of his proposal which made it constitutional was removed over White's objections.

NEXT STEPS

The provision approved today by the committee is similar to the Exon/Coats CDA in that it relies on the "indecency" standard and contains defenses for online service providers. The Senate is likely to adopt the proposal with only minor changes. Senator Exon expressed optimism at today's conference committee meeting that the issue would be resolved soon, perhaps as early as Friday.

The Senate conferees are reviewing the language agreed to today by the House conferees. The House and Senate must each agree on the provisions before the final bill can be voted on. CDT will keep you informed of developments on this issue as they occur.

FOR MORE INFORMATION

Visit CDT's net-censorship issues web page:

http://www.cdt.org/cda.html

---
(2) HOW TO SUBSCRIBE TO THE CDT POLICY POST LIST

CDT Policy Posts, which is what you have just finished reading, are the regular news publication of the Center For Democracy and Technology. CDT Policy Posts are designed to keep you informed on developments in public policy issues affecting civil liberties online.

SUBSCRIPTION INFORMAITON

1. SUBSCRIBING TO THE LIST

To subscibe to the policy post distribution list, send mail to "Majordomo@cdt.org" with:

subscribe policy-posts

in the body of the message (leave the subject line blank)

2. UNSUBSCRIBING FROM THE LIST

If you ever want to remove yourself from this mailing list,
you can send mail to "Majordomo@cdt.org" with the following command
in the body of your email message:

unsubscribe policy-posts youremail@local.host (your name)

(leave the subject line blank)

You can also visit our subscription web page URL:http://www.cdt.org/join.html

---
(3) ABOUT THE CENTER FOR DEMOCRACY AND TECHNOLOGY/CONTACTING US

The Center for Democracy and Technology is a non-profit public interest organization based in Washington, DC. The Center's mission is to develop and advocate public policies that advance constitutional civil liberties and democratic values in new computer and communications technologies.

Contacting us:

General information: info@cdt.org
World Wide Web: URL:http://www.cdt.org
FTP URL:ftp://ftp.cdt.org/pub/cdt/

Snail Mail: The Center for Democracy and Technology
1001 G Street NW Suite 500 East Washington, DC 20001
(v) +1.202.637.9800 (f) +1.202.637.0968

End Policy Post No. 32 12/6/95
