CDT POLICY POST

Number 1

February 9, 1995

A briefing on public policy issues affecting civil liberties online

---

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.

CDT POLICY POST 2/9/95

SUBJECT:
SENATOR EXON INTRODUCES ONLINE INDECENCY LEGISLATION

A. OVERVIEW

Senators Exon (D-NE) and Senator Gorton (R-WA) have introduced legislation to expand current FCC regulations on obscene and indecent audiotext to cover all content carried over all forms of electronic communications networks. If enacted, the "Communications Decency Act of 1995" (S. 314) would place substantial criminal liability on telecommunications service providers (including telephone networks, commercial online services, the Internet, and independent BBS's) if their network is used in the transmission of any indecent, lewd, threatening or harassing messages. The legislation is identical to a proposal offered by Senator Exon last year which failed along with the Senate Telecommunications reform bill (S. 1822, 103rd Congress, Sections 801 - 804). The text of the proposed statute, with proposed amendment, is appended at the end of this document.

The bill would compel service providers to chose between severely restricting the activities of their subscribers or completely shutting down their email, Internet access, and conferencing services under the threat of criminal liability. Moreover, service providers would be forced to closely monitor every private communication, electronic mail message, public forum, mailing list, and file archive carried by or available on their network, a proposition which poses a substantial threat to the freedom of speech and privacy rights of all American citizens.

S. 314, if enacted, would represent a tremendous step backwards on the path to a free and open National Information Infrastructure. The bill raises fundamental questions about the ability of government

to control content on communications networks, as well as the locus of liability for content carried in these new communications media.

To address this threat to the First Amendment in digital media, CDT is working to organize a broad coalition of public interest organizations including the ACLU, People For the American Way, and Media Access Project, along with representatives from the telecommunications, online services, and computer industries to oppose S. 314 and to explore alternative policy solutions that preserve the free flow of information and freedom of speech in the online world. CDT believes that technological alternatives which allow individual subscribers to control the content they receive represent a more appropriate approach to this issue.

B. SUMMARY AND ANALYSIS OF S. 314

S. 314 would expand current law restricting indecency and harassment on telephone services to all telecommunications providers and expand criminal liability to all content carried by all forms of telecommunications networks. The bill would amend Section 223 of the Communications Act (47 U.S.C. 223), which requires carriers to take steps to prevent minors from gaining access to indecent audiotext and criminalizes harassment accomplished over interstate telephone lines. This section, commonly known as the Helms Amendment (having been championed by Senator Jesse Helms), has been the subject of extended constitutional litigation in recent years.

CARRIERS LIABLE FOR CONDUCT OF ALL USERS ON THEIR NETWORKS

S. 314 would make telecommunication carriers (including telephone companies, commercial online services, the Internet, and BBS's) liable for every message, file, or other content carried on its network -- including the private conversations or messages exchanged between two consenting individuals.

Under S. 314, anyone who "makes, transmits, or otherwise makes available any comment, request, suggestion, proposal, image, or other communication" which is "obscene, lewd, lascivious, filthy, or indecent" using a "telecommunications device" would be subject to a fine of $100,000 or two years in prison (Section (2)(a)).

In order to avoid liability under this provision, carriers would be forced to pre-screen all messages, files, or other content before transmitting it to the intended recipient. Carriers would also be forced to prevent or severely restrict their subscribers from communicating with individuals and accessing content available on other networks.

Electronic communications networks do not contain discrete boundaries. Instead, users of one service can easily communicate with and access content available on other networks. Placing the onus, and criminal liability, on the carrier as opposed to the originator of the content, would make the carrier legally responsible not only for the conduct of its own subscribers, but also for content generated by subscribers of other services.

This regulatory scheme clearly poses serious threats to the free flow of information throughout the online world and the free speech and privacy rights of individual users. Forcing carriers to pre-screen content would not only be impossible due to the sheer volume of messages, it would also violate current legal protections.

CARRIERS REQUIRED TO ACT AS PRIVATE CENSOR OF ALL PUBLIC FORUMS AND ARCHIVES

S. 314 would also expand current restrictions on access to indecent telephone audiotext services by minors under the age of 18 to cover similar content carried by telecommunications services (such as America Online and the Internet). (Sec (a)(4)).

As amended by this provision, anyone who, "by means of telephone or telecommunications device, makes, transmits, or otherwise makes available (directly or by recording device) any indecent communication for commercial purposes which is available to any person under the age of 18 years of age or to any other person without that person's consent, regardless of whether the maker of such communication placed the call or initiated the communication" would be subject of a fine of $100,000 or two years in prison.

This would force carries to act as private censors of all content available in public forums or file archives on their networks. Moreover, because there is no clear definition of indecency, carriers would have to restrict access to any content that could be possibly construed as indecent or obscene under the broadest interpretation of the term. Public forums, discussion lists, file archives, and content available for commercial purposes would have to be meticulously screened and censored in order to avoid potential liability for the carrier.

Such a scenario would severely limit the diversity of content available on online networks, and limit the editorial freedom of independent forum operators.

ADDITIONAL NOTABLE PROVISIONS

AMENDMENT TO ECPA

Section (6) of the bill would amend the Electronic Communications Privacy Act (18 USC 2511) to prevent the unauthorized interception and disclosure of "digital communications" (Sec. 6). However, because the term "digital communication" is not defined and 18 USC 2511 currently prevents unauthorized interception and disclosure of "electronic communications" (which includes electronic mail and other forms of communications in digital form), the effect of this provision has no clear importance.

CABLE OPERATORS MAY REFUSE INDECENT PUBLIC ACCESS PROGRAMMING

Finally, section (8) would amend sections 611 and 612 of the Communications Act (47 USC 611 - 612) to allow any cable operator to refuse to carry any public access or leased access programming which contains "obscenity, indecency, or nudity".

C. ALTERNATIVES TO EXON: RECOGNIZE THE UNIQUE USER CONTROL CAPABILITIES OF INTERACTIVE MEDIA

Government regulation of content in the mass media has always been considered essential to protect children from access to sexually- explicit material, and to prevent unwitting listeners/views from being exposed to material that might be considered extremely distasteful. The choice to protect children has historically been made at the expense of the First Amendment ban on government censorship. As Congress moves to regulate new interactive media, it is essential that it understand that interactive media is different than mass media. The power and flexibility of interactive media offers a unique opportunity to enable parents to control what content their kids have access to, and leave the flow of information free for those adults who want it. Government control regulation is simply not needed to achieve the desired purpose.

Most interactive technology, such as Internet browsers and the software used to access online services such as America Online and Compuserve, already has the capability to limit access to certain types of services and selected information. Moreover, the electronic program guides being developed for interactive cable TV networks also provide users the capability to screen out certain channels or ever certain types of programming. Moreover, in the online world, most content (with the exception of private communications initiated by consenting individuals) is transmitted by request. In other words, users must seek out the content they receive, whether it is by joining a discussion or accessing a file archive. By its

nature, this technology provides ample control at the user level. Carriers (such as commercial online services, Internet service providers) in most cases act only as "carriers" of electronic transmissions initiated by individual subscribers.

CDT believes that the First Amendment will be better served by giving parents and other users the tools to select which information they (and their children) should have access to. In the case of criminal content the originator of the content, not the carriers, should be responsible for their crimes. And, users (especially parents) should be empowered to determine what information they and their children have access to. If all carriers of electronic communications are forced restrict content in order to avoid criminal liability proposed by S. 314, the First Amendment would be threatened and the usefulness of digital media for communications and information dissemination would be drastically limited.

D. NEXT STEPS

The bill has been introduced and will next move to the Senate Commerce Committee, although no Committee action has been scheduled. Last year, a similar proposal by Senator Exon was approved by the Senate Commerce committee as an amendment to the Senate Telecommunications Bill (S. 1822, which died at the end of the 103rd Congress). CDT will be working with a wide range of other interest groups to assure that Congress does not restrict the free flow of information in interactive media.

For more information contact:

Daniel Weitzner, CDT Deputy Director (djw@cdt.org)

Jonah Seiger, CDT Policy Analyst (jseiger@cdt.org)

+1.202.637.9800

TEXT OF 47 U.S.C. 223 AS AMENDED BY S. 314

NOTE: [] = deleted
ALL CAPS = additions

47 USC 223 (1992)

Sec. 223. [Obscene or harassing telephone calls in the District of Columbia or in interstate or foreign communications]

OBSCENE OR HARASSING UTILIZATION OF TELECOMMUNICATIONS DEVICES AND FACILITIES IN THE DISTRICT OF COLUMBIA OR IN INTERSTATE OR FOREIGN COMMUNICATIONS"

(a) Whoever--

(1) in the District of Columbia or in interstate or foreign communication by means of [telephone] TELECOMMUNICATIONS DEVICE--

(A) [makes any comment, request, suggestion or proposal] MAKES, TRANSMITS, OR OTHERWISE MAKES AVAILABLE ANY COMMENT,REQUEST, SUGGESTION, PROPOSAL, IMAGE, OR OTHER COMMUNICATION which is obscene, lewd, lascivious, filthy, or indecent;

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

"(B) MAKES A TELEPHONE CALL OR UTILIZES A TELECOMMUNICATIONS DEVICE, WHETHER OR NOT CONVERSATION OR COMMUNICATIONS 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, during which conversation ensues, solely 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,

(2) knowingly permits any [telephone facility] TELECOMMUNICATIONS FACILITY under his control to be used for any purpose prohibited by this section, shall be fined not more than $[50,000]100,000 or imprisoned not more than [six months] TWO YEARS, or both.

(b)(1) Whoever knowingly--

(A) within the United States, by means of [telephone] TELECOMMUNICATIONS DEVICCE, makes (directly or by recording device) any obscene communication for commercial purposes to any person, regardless of whether the maker of such communication placed the call or INITIATED THE COMMUNICATION; or

(B) permits any [telephone facility] TELECOMMUNICATIONS FACILITY under such person's control to be used for an activity prohibited by subparagraph (A), shall be fined in accordance with title 18, United States Code, or imprisoned not more than two years, or both.

(2) Whoever knowingly-- (A) within the United States, [by means of telephone], makes BY MEANS OF TELEPHONE OR TELECOMMUNICATIONS DEVICE, MAKES, TRANSMITS, OR MAKES AVAILABLE(directly or by recording device) any indecent communication for commercial purposes which is available to any person under 18 years of age or to any other person without that person's consent, regardless of whether the maker of such communication placed the call OR INITIATED THE COMMUNICATION; or

(B) permits any [telephone facility] TELECOMMUNICATIONS FACILITY under such person's control to be used for an activity prohibited by subparagraph (A), shall be fined not more than $[50,000] 100,000 or imprisoned not more than [six months] TWO YEARS, or both.

(3) It is a defense to prosecution under paragraph (2) of this subsection that the defendant restrict access to the prohibited communication to persons 18 years of age or older in accordance with subsection (c) of this section and with such procedures as the Commission may prescribe by regulation.

(4) In addition to the penalties under paragraph (1), whoever, within the United States, intentionally violates paragraph (1) or (2) shall be subject to a fine of not more than $[50,000] 100,000 for each violation. For purposes of this paragraph, each day of violation shall constitute a separate violation.

(5)(A) In addition to the penalties under paragraphs (1), (2), and (5), whoever, within the United States, violates paragraph (1) or (2) shall be subject to a civil fine of not more than $[50,000] 100,000 for each violation. For purposes of this paragraph, each day of violation shall constitute a separate violation.

(B) A fine under this paragraph may be assessed either--

(i) by a court, pursuant to civil action by the Commission or any attorney employed by the Commission who is designated by the Commission for such purposes, or

(ii) by the Commission after appropriate administrative proceedings.

(6) The Attorney General may bring a suit in the appropriate district court of the United States to enjoin any act or practice which violates paragraph (1) or (2). An injunction may be granted in accordance with the Federal Rules of Civil Procedure.

(c)(1) A common carrier within the District of Columbia or within any State, or in interstate or foreign commerce, shall not, to the extent technically feasible, provide access to a communication specified in subsection (b) from the telephone of any subscriber who has not previously requested in writing the carrier to provide access to such communication if the carrier collects from subscribers an identifiable charge for such communication that the carrier remits, in whole or in part, to the provider of such communication.

(2) Except as provided in paragraph (3), no cause of action may be brought in any court or administrative agency against any common carrier, or any of its affiliates, including their officers, directors, employees, agents, or authorized representatives on account of--

(A) any action which the carrier demonstrates was taken in good faith to restrict access pursuant to paragraph (1) of this subsection; or

(B) any access permitted--

(i) in good faith reliance upon the lack of any representation by a provider of communications that communications provided by that provider are communications specified in subsection (b), or

(ii) because a specific representation by the provider did not allow the carrier, acting in good faith, a sufficient period to restrict access to communications described in subsection (b).

(3) Notwithstanding paragraph (2) of this subsection, a provider of communications services to which subscribers are denied access pursuant to paragraph (1) of this subsection may bring an action for a declaratory judgment or similar action in a court. Any such action shall be limited to the question of whether the communications which the provider seeks to provide fall within the category of communications to which the carrier will provide access only to subscribers who have previously requested such access.

CDT POLICY POST

Number 2

February 13, 1995

A briefing on public policy issues affecting civil liberties online

---

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.

CDT POLICY POST 02/13/95

CONTENTS:

X9 COMMITTEE AGREES TO DEVELOP 3x DES ENCRYPTION STANDARD

Major Setback for NSA

The NSA's efforts to push the adoption the Clipper/Skipjack government- escrowed encryption scheme encountered a major setback earlier this month with the decision by the Accredited Standards Committee X9 to proceed with the development of a data security standard based on triple-DES.

The ASC X9 committee is responsible for setting data security standards for the US banking and financial services industries. These industries are heavy users of commercial cryptography, and standards developed for this community tend to drive the development of applications for the entire market. As a result, the committee's decision to proceed with a triple-DES standard has important implications for future cryptographic standards and US cryptography policy generally.

The NSA, a voting member of the X9 committee, had lobbied hard against the proposal. In a November letter to committee members, the NSA threatened to prevent the export of triple- DES, citing existing US law and potential threats to national security (see attached NSA letter).

The decision sets the stage for the development of a next generation of security standards based on publicly available, non-escrowed encryption schemes. A battle over the exportability of triple-DES applications is also on the horizon.

Through export controls on cryptography, the proposed Clipper initiative, and interference in the standards setting processes, US government policies have consistently sought to make strong encryption and other privacy protecting technologies unavailable to the general public. The X9 decision and development of triple-DES and other alternitives to government-escrowed cryptography is an important victory in that it will increase the public's access to strong, privacy enhancing technologies.

BACKGROUND

Banks and other financial institutions use encryption to protect the billions of dollars in transactions and fund transfers which flow every day across the world's communications networks.

The current encryption standard used by the banking industry is based on DES, which has been available since the early 1970's. DES is widely trusted because it has been repeatedly tested and is considered by experts to be unbreakable except by brute force (trying every possible key combination). The US government has also allowed the limited export of DES.

Despite its popularity, DES is considered to be reaching the end of its useful life. The increasing speed and sophistication of computer processing power has begun to render DES vulnerable to brute force attacks. Cryptographers have recently demonstrated that DES codes can be cracked in as little as three hours with $1 million worth of currently available equipment. As a result, the banking and financial services industries have begun to explore alternatives to DES.

Although there are many potential alternatives to DES, triple-DES is widely seen as the most practical solution. Triple-DES is based on DES, but has been enhanced by increasing the key length and by encrypting through multiple iterations. These enhancements make triple-DES less vulnerable to brute force attacks. Triple-DES is also popular because it can be easily incorporated into existing DES systems and is based on standards and procedures familiar to most users.

NSA SETBACK IS A VICTORY FOR CLIPPER OPPONENTS

In their November letter to X9 committee members, the NSA attempted to undermine the attractiveness of triple-DES by arguing that it is cryptographically unsound, a potential threat to national security, and would not be exportable under US law. The NSA, while offering no specific alternative to triple-DES, seemed to be attempting to push the committee to adopt the only currently available option -- Clipper.

Privacy advocates also lobbied the X9 committee. In a letter sent in advance of the December 1994 ballot, CDT Deputy Director Daniel Weitzner (then EFF Deputy Policy Director) and EFF board member John Gilmore, an expert in this field, sent a letter to X9 committee members urging them to adopt the triple-DES standard. A copy of the letter is appended at the end of this post.

By agreeing to develop a triple-DES standard, the X9 committee has clearly and decisively rejected Clipper as a solution. This vote thus represents a further repudiation to Clipper and yet another victory for opponents of government efforts to establish Clipper or other government-escrowed solutions as a national standard.

NEXT STEPS

X9F, a subcommittee of the X9 committee, will now develop technical standards for implementing triple-DES based applications. This process is expected to take one or two years to complete. Once technical standards are developed, the full X9 committee will vote as to whether to implement the subcommittee's technical recommendations.

The availability of triple-DES applications received a further boost recently with the announcement by AT&T and VLSI Technologies that they were developing new data security products based on triple-DES. This will presumably provide additional options for X9 committee members, but the exportability of these products is still in doubt.

The stage is thus set for a further battle between the NSA and the X9 committee over the exportability of triple-DES and final approval of the X9 standard. As a sitting member of the committee, NSA will presumably continue to lobby against efforts by the committee to develop triple-DES applications. Furthermore, the banking and financial services industries must still persuade the government to allow for the export of triple- DES.

As an opponent of government-escrowed cryptography, CDT applauds the recent actions of the X9 committee. While CDT supports the development of a variety of security standards and alternatives to DES, we recognize the need of the banking and financial services industries to develop temporary stop-gap solution. CDT will continue to work towards the relaxation of export controls on cryptography and will support X9 committee members in their efforts to gain the ability to export triple- DES applications.

For more information contact:

Daniel J. Weitzner, Deputy Director (djw@cdt.org)
Jonah Seiger, Policy Analyst (jseiger@cdt.org)

+1.202.637.9800

GILMORE/WEITZNER LETTER TO X9 COMMITTEE MEMBERS

November 18, 1994

Dear Accredited Standards Committee-X9 Member:

The X9 Committee is currently voting as to whether to recommend the development of a standard for triple-DES (ballot number X9/94-LB#28). The Electronic Frontier Foundation (EFF) strongly urges you to vote in favor of the triple-DES standard.

EFF supports the development of a variety of new data security standards and alternatives to DES. We believe the triple-DES standard provides the best immediate short term alternative because:

- The basic algorithm, DES, is strong and has been tested repeatedly.
- There are no known attacks that succeed against triple-DES.

- It is clearly no less secure than DES.
- It eliminates the brute-force problem completely by tripling the key length.
- It runs at high speeds in easy-to-build chips.
- It can be easily incorporated into existing systems.

NSA's opposition to triple-DES appears to be an indirect attempt to push Clipper by eliminating credible alternatives. Clipper is not a viable alternative to triple-DES, and carries substantial liabilities. There has been no evidence of foreign acceptance of the standard and the skipjact algorithm is classified. The likelihood of any government accepting secret standards developed by a foreign security agency is slim. Clinton Administration efforts, through the NSA, to push Clipper as a domestic standard over the past two years have failed.

We urge you to carefully consider the alternatives before you cast your ballot. We believe that the triple-DES issue should be decided on its own merits.

Sincerely,

John Gilmore
Board of Directors
Electronic Frontier Foundation

Daniel J. Weitzner
Deputy Policy Director
Electronic Frontier Foundation

NSA LETTER TO X9 COMMITTEE MEMBERS

X9 Member:

I will be casting a NO vote on the NWI for triple-DES, Letter Ballot X9/94-LB#28. The reasons are set forth below. You may find these useful as you determine your position.

Jerry Rainville

NSA REASONS FOR A NEGATIVE VOTE

While NSA supports the use of DES in the global financial sector, we believe that standardization of triple-DES is ill- advised for a number of reasons.

The financial community should be planning to transition to a new generation of cryptographic algorithms. When DES was first introduced, it represented the "only game in town". It supported encryption, authentication, key management, and secure hashing applications. With a broader interest in security, the market can now support optimized algorithms by application. Going through the expense of installing a stop- gap can only serve to delay progress in achieving interoperable universal appropriate solutions.

While we understand the appeal of a snap-in upgrade, our experience has been that any change is

expensive, especially one where the requirements on the key management system change. We do not agree that replacing DES with triple-DES is significantly less expensive than upgrading to more appropriate technology.

Tripling of any algorithm is cryptographically unsound. Notice that tripling DES, at best, only doubles the length of the cryptovariable (key). Phrased another way, the DES was optimized for security at 56 bits. We cannot vouch that any of the schemes for doubling the cryptovariable length of DES truly squares security.

We understand the financial community has concerns with current key escrow based encryption, however, we are committed to searching for answers to those concerns. But the government is also committed to key escrow encryption, and we do not believe that the proposal for triple DES is consistent with this objective.

US export control policy does not allow for general export of DES for encryption, let alone triple-DES. Proceeding with this NWI would place X9 at odds with this long standing policy. It also violates the newly accepted X9 cryptographic policy.

The US government has not endorsed triple-DES; manufacturers and users may be reluctant to use triple-DES products for fear of possible liability.

Finally, further proliferation of triple-DES is counter to national security and economic objectives. We would welcome the opportunity to discuss these concerns with an appropriate executive of your institution.

ABOUT THE CENTER FOR DEMOCRACY AND TECHNOLOGY

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)

CDT POLICY POST

Number 3

March 3, 1995

A briefing on public policy issues affecting civil liberties online

---

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.

CDT POLICY POST 2/9/95

CONTENTS:

CDT LED COALITION SENDS LETTER TO SENATORS EXON AND PRESSLER

MESSAGE: REMOVE S. 314 FROM FAST TRACK

The Interactive Working Group (a coalition of public interest organizations, members of the computer and communications industry, and associations representing librarians and the press, chaired by the Center For Democracy and Technology) today sent a letter to Senators Pressler, Exon, and the Senate

Commerce Committee. The letter expresses serious concerns about S. 314 (the "Communications Decency Act of 1995") from the standpoint of the First Amendment and the viability of the entire communications industry. Because of these and other concerns, the coalition asked Senator Pressler and Exon not to incorporate S. 314 into Senate telecommunications reform legislation which is expected to be introduced later this month.

The letter and a list of signatories are attached below.

S. 314 would expand current law restricting indecency and harassment on telephone services to all telecommunications providers and expand criminal liability to all content carried by all forms of telecommunications networks. The bill would amend Section 223 of the Communications Act (47 U.S.C. 223), which requires carriers to take steps to prevent minors from gaining access to indecent audiotext and criminalizes harassment accomplished over interstate telephone lines.

If enacted, S. 314 would compel service providers to severely restrict your online activities. Your access to email, discussion lists, usenet, the world wide web, gopher, and ftp archives would be substantially reduced or cut off entirely. The bill would also force providers to closely monitor and pre-screen your electronic mail, and refuse to transmit any message or other content which may be considered to be indecent.

This bill poses a significant threat to freedom of speech and the free flow of information in cyberspace. The bill also raises fundamental questions about the right of government to control content on communications networks, as well as the locus of liability for content carried in these new communications media.

INTERACTIVE WORKING GROUP LETTER

March 2, 1995

Chairman Larry Pressler
Senate Commerce Committee
United States Senate Washington, DC

Senator James Exon
United States Senate
528 Hart Senate Office Building
Washington, DC

Dear Chairman Pressler and Senator Exon:

We write regarding the Communications Decency Act of 1995 (S. 314), introduced recently by Senator James Exon and Senator Slade Gorton. We request that such legislation not be considered as part of the fast track telecommunications reform measure now before the Commerce Committee. The undersigned members of the computer and communications industry, the press, and the public interest community believe that this legislation raises fundamental questions regarding the involvement of government in content regulation in new interactive media.

Developing means for detecting and holding wrong-doers responsible for illegal activity, and permitting parents to control access by their children to adult material while still preserving our constitutional

liberties, are important goals shared by many in our society. However, the choice of methods for achieving these goals raises serious free speech and censorship problems. Our commitment is to work with you and your colleagues to resolve these issues in ways which will enable individual and parental choice, without impairing the free flow of information or stifling development of emerging technology through bureaucratic regulation.

In recognition of the seriousness of these issues, the undersigned organizations have formed a working group to identify legal and regulatory options that maximize parental control, individual accountability, and the free flow of information in new communication technologies. We are encouraged that new interactive communications technologies -- including online services and interactive television offered by cable, telephone companies, and others in the public sector -- already offer technological means to give consumers choice over the content that they receive and enable parents to control access to controversial material. Many more such features are in development. Market signals already indicate to those of us who are building the Information Superhighway that users want choice of programming and control over the materials to which their children are exposed. Information providers in the public and private sector are working to meet these needs.

We plan to devote intensive effort toward developing comprehensive solutions to the problems raised by S. 314. Desirable solutions will take advantage of the empowering potential of new technology for increased user control over programming and information content. However, we must emphasize that we strongly disagree with the approach embodied in this legislation that would in effect require those who merely provide the means of transmitting messages to censor the content of such materials, as well as become liable for the criminal actions of others based solely on the content of the messages transmitted. Applying the regulatory models developed for today's mass media to the interactive media of tomorrow, will only serve to thwart the development of new media.

In the coming year, we hope to have the opportunity to work diligently with you and other policy makers to assure that the empowering potential of interactive media is achieved, and to arrive at comprehensive, forward looking solutions to the issues before us without jeopardizing fundamental First Amendment values.

Sincerely,

American Civil Liberties Union
America Online, Inc.
Association of Research Libraries
American Society of Newspaper Editors
American Association of Law Librarians
American Library Association
Apple Computer
Business Software Alliance
Cavanagh Associates
Center for Democracy and Technology
Compuserve Incorporated
Consumer Federation of America
Cox Enterprises, Inc
Electronic Frontier Foundation
Electronic Messaging Association
Information Technology Industry Council
Interactive Services Association
Media Access Project
Newspaper Association of America
National Newspaper Association

National Retail Federation
People for the American Way Action Fund
Recreational Software Advisory Council
SmithKline Beecham
Software Publishers Association
Targetbase Marketing
The Internet Company
Time Warner

cc: Members, Senate Commerce Committee

FOR MORE INFORMATION ON S. 314 AND WHAT YOU CAN DO

HELP *STOP* S.314 Send a letter or call your Senator! For information on how you can help, send a message to vtw@vtw.org.

DOCUMENTS

CDT's analysis of S. 314 and the text of the bill can be obtained at the Voters Telecommunications Watch (VTW) archive:

WWW URL: gopher://gopher.panix.com/11/vtw/exon

Gopher command : gopher -p 1/vtw/exon gopher.panix.com

You can also obtain information by sending a message to (s314-info@cdt.org)

ABOUT THE CENTER FOR DEMOCRACY AND TECHNOLOGY

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)

CDT POLICY POST Number 4 3/16/95
A briefing on public policy issues affecting civil liberties online

CONTENTS:

SENATOR LEAHY ASKS CDT LED COALITION TO EXPLORE ALTERNATIVES TO S. 314

Senator Patrick Leahy (D-VT), a strong proponent of civil liberties and the development of new communications technologies,has raised serious concerns about the Communications Decency Act (S. 314). In a letter to CDT Executive Director Jerry Berman and th e Interactive Working Group, Senator Leahy stated that "The proposed legislative solutions . . . raise serious concerns about the free flow of information in new communications media, threaten to squelch the development of the Internet and a vital new ind ustry along with it."

Senator Leahy has asked the Interactive Working Group (a coalition of public interest organizations, members of the computer and communications industry, and associations representing librarians and the press, chaired by the Center For Democracy and Techn ology) to "explore alternatives that balance constitutional liberties, competitiveness, and the legitimate interest of protecting children from accessing controversial content." The letter is attached below.

Leahy's efforts to explore alternatives to S. 314 come at an important time in this debate over S. 314. The Senate Commerce Committee may still incorporate S. 314 into telecommunications reform legislation, expected to be introduced as early next Monday (3/20).

It is critical that you contact Commerce Committee Chairman Pressler (R- SD), Senator Packwood (R-OR), Senator Hollings (D-SC), and your own Senators and urge them to:

- Take S. 314 off the fast track,
- Keep S. 314 out of the Senate telecommunications reform legislation, and,
- Support Senator Leahy's effort to explore alternatives that are consistent with the First Amendment and the free flow of information.

For more information on how to contact members of congress, send email to the Voter's Telecommunications Watch vtw@vtw.org.

While you are at it, you might send a note of thanks to Senator Leahy for his efforts on behalf of free speech and the free flow of information in cyberspace. He can be reached by email at senator_leahy@leahy.senate.gov

The Center for Democracy and members of the Interactive Working Group are grateful to Senator Leahy for his leadership on this issue and his willingness to explore the implications of government efforts to impose content regulations on interactive media.

SENATOR LEAHY'S LETTER TO INTERACTIVE WORKING GROUP

March 15, 1995

Mr. Jerry Berman
Interactive Working Group
Center for Democracy and Technology
1001 G St., NW
Suite 700 East
Washington, DC 2000

Dear Mr. Berman:

Interactive communications media are growing at an astonishing rate, promising great advances for domestic commerce, international competitiveness, and political and cultural life. Nearly ten years ago, we began work on the Electronic Communications Priva cy Act ("ECPA"), in recognition of the fact that new computer and communications technologies would only flourish in an environment where the privacy rights of users, the intellectual property rights of content providers, and the obligations of service pr oviders are clear under statute. We continued that work last year in the Communications Assistance for Law Enforcement Act ("CALEA"). Today, as interactive communications systems expand in the consumer market, there is a critical need to clarify the First Amendment rights and responsibilities of information providers, users and carriers.

As you know, a number of bills have been introduced in the Senate that would regulate a wide range of controversial content on interactive information services, including the Internet. This legislation is motivated by two important goals. First, parents s hould be able to control their children's access to controversial material. Second, adult users should be able to exercise reasonable control over the information they receive so they may avoid material offense to them. The proposed legislative solutions to achieve these goals raise serious concerns about the free flow of information in new communications media, and threaten to squelch the development of the Internet and a vital new industry along with it.

I understand that industry and public interest organizations have independently come together to form the Interactive Working Group in order to address these issues. My hope is that the group will explore public policy and technology options for addressin g the problems of children's access to obscene content in a manner which promotes parental empowerment and First Amendment values. I would appreciate the Interactive Working group Consideration of and recommendation on the following issues:

1. THE NATIONAL AND INTERNATIONAL INFORMATION INFRASTRUCTURE:

What effect will content regulation have on the development of the national and global information infrastructure, including the Internet and other interactive services?

2. CURRENT LAW AND ENFORCEMENT EFFORTS:

What is the current lawregulating obscenity and harassment online? What gaps, if any, are there in current federal and state laws which hamper prosecution of criminal activity, including violations of the copyright and obscenity laws, in interactive media ?

3. TECHNOLOGICAL SOLUTIONS:

Does interactive technology enable parents to control their children's access to information in online services today? If not, what steps would be required to enable such parental control? Can the Working Group provide demonstrations of these user control technologies?

4. CONSTITUTIONAL FREE SPEECH AND PRIVACY ISSUES:

What are the First Amendment implications of content regulation in interactive media? What is the impact of carrier liability for content on ECPA , CALEA and constitutional privacy protections?

Since the passage of the Electronic Communications Privacy Act, and again in CALEA, we have always worked to assure a proper balance of constitutional liberties, competitiveness and legitimate government interest in the regulation of new communications te chnologies. As I receive input from a number of sources on these important issues, I look forward to your advice as well. My staff is available to meet with members of your group to discuss these issues further.

Sincerely,

[sig]

Patrick J. Leahy United States Senator

FOR MORE INFORMATION ON S. 314 AND WHAT YOU CAN DO

HELP STOP S.314

Send a letter or call your Senator! For information on how you can help, send a message to vtw@vtw.org

DOCUMENTS

CDT's analysis of S. 314 and the text of the bill can be obtained at the Voters Telecommunications Watch (VTW) archive:

WWW URL: gopher://gopher.panix.com/11/vtw/exon

Gopher command : gopher -p 1/vtw/exon gopher.panix.com

You can also obtain information by sending a message to s314-info@cdt.org.

ABOUT THE CENTER FOR DEMOCRACY AND TECHNOLOGY

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 tech nologies.

Contacting us:

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

www/ftp/gopher archives are currently under construction, and should be up and running by the middle of March.

POLICY POST

March 23, 1995
Number 5

CENTER FOR DEMOCRACY AND TECHNOLOGY

A briefing on public policy issues affecting civil liberties online
---
CDT POLICY POST 3/23/95 Number 5

CONTENTS: (1) Exon Indecency Bill Approved by Sen. Commerce Committee
(3) About the Center For Democracy and Technology

EXON INDECENCY BILL APPROVED BY SENATE COMMERCE COMMITTEE

The Senate Commerce Committee voted unanimously today to adopt S. 314, Senator Exon's "Communications Decency Act", as an amendment to the Senate telecommunications reform legislation. The amendment was introduced by Senator Slade Gorton (R-WA) on behalf of himself an Exon (D-NE). It received no significant debate and was unanimously approved on a voice vote.

The bill was amended from its original form to limit liability for telecommunications carriers and online service providers, but users and content providers would still be criminally liable for any communications that are deemed "obscene, lewd, lascivious, filthy, or indecent". An analysis of these provisions by CDT, as well as the full text of the bill will be posted later today.

On initial analysis, CDT still believes that the bill is an unconstitutional violation of the free speech and privacy rights of network users and content providers.

Although the Commerce Committee did vote to send the Telecommunications reform legislation to the Senate floor, there are still serious disputes about the entire package. Because of this, there are still many opportunities to remove the "Indecency Provision" as the bill moves to the floor.

Stay tuned for further analysis and additional information from CDT.

ABOUT THE CENTER FOR DEMOCRACY AND TECHNOLOGY

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

www/ftp/gopher archives are currently under construction, and should be up and running by the end of March.

###

POLICY POST

March 24, 1995
Number 6

CENTER FOR DEMOCRACY AND TECHNOLOGY

A briefing on public policy issues affecting civil liberties online
---
CDT POLICY POST 3/24/95 Number 6

CONTENTS: (1) CDT Analysis of Revised Exon Indecency Legislation
(2) Section 223 as amended by Communications Decency Act
(3) About the Center For Democracy and Technology

CDT ANALYSIS OF REVISED EXON INDECENCY LEGISLATION

I. OVERVIEW

A revised version of the Communications Decency Act (S.314) was added to the Senate telecommunications reform legislation as the reform bill was reported out of the Senate Commerce Committee. In an important improvement over the original version, several exemptions have been created to limit criminal liability of online services providers where they exercise no control over content. However, despite this significant change the bill is still an unconstitutional intrusion of the free speech and privacy rights of Internet users and all content providers in interactive media. (The complete text of the bill interleaved into the current statute is attached at the end of this Policy Post.)

In simple terms, the Communications Decency Act would enshrine in statute a sharp distinction between the print medium and new interactive media. The bill subjects interactive media to the same weak First Amendment protections that have evolved for mass media. Moreover, it places all speech that occurs on the Internet and elsewhere in cyberspace under the jurisdiction of the Federal Communications Commission. Both the interactive media and the print media are arenas in which individuals and organizations exercise core First Amendment free speech rights. Thus, new interactive media -- which includes not only email and Internet servicese, but also interactive TV, video on demand and distance learning -- must be protected by the First Amendment.

The Center for Democracy and Technology (CDT) remains actively opposed to this

bill. With the help of Senator Leahy and other civil liberties advocates in Congress, we will fight to keep it from being enacted and continue to search for alternatives to this dangerous legislation. CDT believes that federal legislation is needed to solidify free speech rights and clarify online service provider liability. Without such legislation, a series of state legislative proposed as bad or worse than the Exon/Gorton bill will proliferate. Restrictive proposals already under consideration in states such as Maryland, Oregon, and Washington must be pre-empted. We will work with concerned legislators and the Interactive Working Group (an ad hoc coalition of public interest organizations, and computer, communication, and publishing firms) to develop alternatives.

II. ANALYSIS OF CURRENT PROPOSAL

The Exon/Gorton bill was introduced to promote the important purpose of protecting minors from access to controversial and inappropriate sexually explicit material in interactive media including the Internet, other commercial online services, electronic bulletin board services (BBS's). However, because the proposed statute is grafted onto a twenty five year-old provision of the Communications Act which was designed for a centralized monopoly telephone environment, instead of diverse, decentralized interactive media, it both fails to accomplish its goal and is unconstitutional on its face. In spite of the changes made by Senator Exon, the bill still suffers the following critical defects from the standpoint of users and content providers:

1. SECOND CLASS FIRST AMENDMENT RIGHTS FOR USERS AND CONTENT PROVIDERS ON THE NET AND ALL INTERACTIVE MEDIA: Even though many laud cyberspace as the new electronic gutenberg printing press accessible to all, the Exon bill treats the Internet, interactive television, and video dialtone systems as if they were one big radio station whose broadcasts are constantly assaulting unwilling listeners. Those who use these new technologies know that this is not the case. However, viewing interactive media as an extension of broadcasting diminishes the First Amendment rights of all who use these systems and create content for them. 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 if this legislation is enacted.

2. FEDERAL COMMUNICATIONS COMMISSION JURISDICTION OVER ONLINE SPEECH: The defenses to prosecution established in the new version of the bill gives the Federal Communications Commission jurisdiction to establish rules governing distribution of content online. This will have a dramatic chilling effect on online activity and squelch the development of interactive media. Regulation of indecency in this new medium is a bad precedent for all kinds of speech in the interactive world.

3. CRIMINALIZATION OF BOTH PUBLIC AND PRIVATE MESSAGES THAT ARE NOT OBSCENE: The Act criminalizes not only obscene, but also "lewd, lascivious, filthy, or indecent" communications, all of which are protected by the First Amendment and cannot be banned.

4. IMPERMISSIBLY INTRUSIVE MEANS OF ACHIEVING LEGITIMATE GOAL: First Amendment jurisprudence requires that restrictions on speech adopt the "least restrictive means" available for achieving a compelling purpose. Relying on technological assumptions applicable only to 900 number services and a centrally-controlled telephone system, the Act fails to account for the fact that government restriction on content is unnecessary in interactive media, where parents can control the content that their children access.

5. FAULTY ANALOGY TO BROADCAST MEDIA: Proponents of the Act have justified the constitutionality by improper reliance on content restrictions found acceptable in broadcast media. These arguments fail to recognize that while broadcast media may "assult" unwilling listeners, who may be in need of government protection, interactive media enables users to control the information that they receive.

6. INVASION OF PRIVACY: By criminalizing the content of private, non-obscene messages, the Act would force an invasion of the realm of private electronic communications and end the individual's ability to control the content of information he or she chooses to access in private.

Alternative means of achieving the goal of protecting minors from access to material considered inappropriate by their parents would include:

1. FEDERAL LEGISLATION ESSENTIAL TO PROTECT FREE SPEECH ON THE NET: CDT believes that there mujst be federal legislation to solidify free speech rights and clarify carrier liability which pre-empts state legislation in this area. Otherwise, as series of state legislative proposed where are as bad or worse than the Exon/Gorton bill will proliferate.

2. MAXIMUM RELIANCE ON TECHNOLOGY TO EMPOWER PARENTS: Interactive media offers parents and other users the ability to filter certain kinds of content. Instead of relying on government censorship, or even government-imposed rating systems, parents should be able to block the delivery of certain information to their children on the basis of their own individual tastes and preferences.

3. CLEAR PROTECTION FOR CONSTITUTIONALLY-PERMISSIBLE SPEECH: Any alternative legislation must provide affirmative protection for constitutionally-permissible speech, even if it is lewd, filthy or otherwise controversial. The First Amendment demands that offensive or disturbing speech must be treated separately than that which is clearly obscene and unprotected.

4. EMPHASIS ON ENFORCEMENT OF EXISTING STATUTES: Federal and state law already prohibits transportation of obscenity, child pornography, as well as, in many instances threats, stalking and harassment. To the extent that there are obstacles to enforcing these laws in the new on-line environment, Congress should examine whether new law is required, or whether more resources for enforcement (including training for law enforcement in interactive services and cooperative efforts with the

industry).

5. CODIFICATION SEPARATELY FROM EXISTING DIAL-A-PORN STATUTE:
Modification of the existing ¤ 223, originally written for the analogue telephone system, to regulate new interactive media causes unnecessary confusion, both for the treatment of the new technology and with respect to the stability of the regulation of audiotext services. If new is written, it should stand on its own. Moreover, Congress should consider which elements properly belong in the Communications Act and which in the Criminal Code.

The regulation of speech, commerce, and privacy rights in new interactive communications systems raises many difficult issues of public policy and constitutional law. Before proceeding with legislation, Congress must provide the opportunity for public hearings to identify clearly the problems that exist, and to identify solutions that are appropriate to the new technology. Failure to do so will result in ineffective policy, years of constitutional litigation, and a disastrous chilling effect on the development and growth of a very promising new communications medium.

For More Information Contact:

Center for Democracy and Technology

Jerry Berman <jberman@cdt.org>
Daniel Weitzner <djw@cdt.org>
(voice) +1.202.637.9800

TEXT OF STATUTE WITH PROPOSED AMENDMENT:

Substantial changes from previous version include:

-- the term 'knowingly' has been added to section (a)(1)(A)
-- additional defenses have been added in subsection (d)

NOTE: [] = deleted
ALL CAPS = additions

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]

OBSCENE OR HARASSING UTILIZATION OF TELECOMMUNICATIONS DEVICES AND FACILITIES IN THE DISTRICT OF COLUMBIA OR IN

INTERSTATE OR FOREIGN COMMUNICATIONS"

(a) Whoever--

(1) in the District of Columbia or in interstate or foreign communication by means of [telephone] TELECOMMUNICATIONS DEVICE--

[(A) makes any comment, request, suggestion or proposal which is obscene, lewd, lascivious, filthy, or indecent;]

(A) 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;

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

(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, during which conversation ensues, solely to harass any person at the called number; or

(2) knowingly permits any [telephone] TELECOMMUNICATIONS facility under his control to be used for any purpose prohibited by this section, shall be fined not more than $[50,000]100,000 or imprisoned not more than [six months] TWO YEARS, or both.

(b)(1) Whoever knowingly--

[(A) within the United States, by means of telephone, makes (directly or by recording device) any obscene communication for commercial purposes to any person, regardless of whether the maker of such communication placed the call;]

(A) WITHIN THE UNITED STATES, BY MEANS OF TELECOMMUNICATIONS DEVICE --

(i) MAKES, CREATES, OR SOLICITS, AND
(ii) PURPOSEFULLY MAKES AVAILABLE,

ANY OBSCENE COMMUNICATION FOR COMMERCIAL PURPOSES TO ANY PERSON, REGARDLESS OF
WHETHER THE MAKER OF SUCH COMMUNICATION PLACED THE CALL OR INITIATED THE COMMUNICATION; OR

(B) permits any [telephone facility] TELECOMMUNICATIONS

FACILITY under such person's control to be used for an activity prohibited by subparagraph (A), shall be fined in accordance with title 18, United States Code, or imprisoned not more than two years, or both.

(2) Whoever knowingly--

[(A) within the United States, by means of telephone, makes (directly or by recording device) any indecent communication for commercial purposes which is available to any person under 18 years of age or to any other person withoutthat person's consent, regardless of whether the maker of such communication placed the call; or]

(A) WITH THE UNITED STATES, BY MEANS OF TELEPHONE OR TELECOMMUNICATIONS DEVICE,

(i) MAKES, CREATES, OR SOLICITS, AND
(ii) PURPOSEFULLY MAKES AVAILABLE (DIRECTLY OR BY RECORDING DEVICE)

ANY INDECENT COMMUNICATIONS FOR COMMERCIAL PURPOSES WHICH IS AVAILABLE TO ANY
PERSON UNDER 18 YEARS OF AGE OR TO ANY OTHER PERSON WITHOUT THAT PERSON'S CONSENT, REGARDLESS OF WHETHER THE MAKER OF SUCH COMMUNICATION PLACED THE CALL; OR

(B) permits any [telephone facility] TELECOMMUNICATIONS FACILITY under such person's control to be used for an activity prohibited by subparagraph (A), shall be fined not more than $[50,000] 100,000 or imprisoned not more than [six months] TWO YEARS, or both.

(3) It is a defense to prosecution under paragraph (2) of this subsection that the defendant restrict access to the prohibited communication to persons 18 years of age or older in accordance with subsection (c) of this section and with such procedures as the Commission may prescribe by regulation.

(4) In addition to the penalties under paragraph (1), whoever, within the United States, intentionally violates paragraph (1) or (2) shall be subject to a fine of not more than $[50,000] 100,000 for each violation. For purposes of this paragraph, each day of violation shall constitute a separate violation.

(5)(A) In addition to the penalties under paragraphs (1), (2), and (5), whoever, within the United States, violates paragraph (1) or (2) shall be subject to a civil fine of not more than $[50,000] 100,000 for each violation. For purposes of this paragraph, each day of violation shall constitute a separate violation.

(B) A fine under this paragraph may be assessed either--

(i) by a court, pursuant to civil action by the Commission or any attorney employed by the Commission who is designated by the

Commission for such purposes, or

(ii) by the Commission after appropriate administrative proceedings.

(6) The Attorney General may bring a suit in the appropriate district court of the United States to enjoin any act or practice which violates paragraph (1) or (2). An injunction may be granted in accordance with the Federal Rules of Civil Procedure.

(c)(1) A common carrier within the District of Columbia or within any State, or in interstate or foreign commerce, shall not, to the extent technically feasible, provide access to a communication specified in subsection (b) from the [telephone] TELECOMMUNICATIONS DEVICE of any subscriber who has not previously requested in writing the carrier to provide access to such communication if the carrier collects from subscribers an identifiable charge for such communication that the carrier remits, in whole or in part, to the provider of such communication.

(2) Except as provided in paragraph (3), no cause of action may be brought in any court or administrative agency against any common carrier, or any of its affiliates, including their officers, directors, employees, agents, or authorized representatives on account of--

(A) any action which the carrier demonstrates was taken in good faith to restrict access pursuant to paragraph (1) of this subsection; or

(B) any access permitted--

(i) in good faith reliance upon the lack of any representation by a provider of communications that communications provided by that provider are communications specified in subsection (b), or

(ii) because a specific representation by the provider did not allow the carrier, acting in good faith, a sufficient period to restrict access to communications described in subsection (b).

(3) Notwithstanding paragraph (2) of this subsection, a provider of communications services to which subscribers are denied access pursuant to paragraph (1) of this subsection may bring an action for a declaratory judgment or similar action in a court. Any such action shall be limited to the question of whether the communications which the provider seeks to provide fall within the category of communications to which the carrier will provide access only to subscribers who have previously requested such access.

(d) ADDITIONAL DEFENSES; RESTRICTIONS ON ACCESS; JUDICIAL REMEDIES RESPECTING RESTRICTIONS. --

(1) NO PERSON SHALL BE HELD TO HAVE VIOLATED THIS SECTION
WITH RESPECT TO ANY ACTION BY THAT PERSON OR A SYSTEM UNDER HIS CONTROL
THAT IS LIMITED SOLELY TO THE PROVISION OF ACCESS, INCLUDING TRANSMISSION,
DOWNLOADING, INTERMEDIATE STORAGE, NAVIGATIONAL TOOLS, AND RELATED
CAPABILITIES NOT INVOLVING THE CREATION OR ALTERATION OF THE CONTENT OF THE
COMMUNICATIONS, FOR OTHER
PERSON'S COMMUNICATIONS TO OR FROM A SERVICE, FACILITY, SYSTEM, OR NETWORK NOT

UNDER THAT PERSON'S CONTROL.

(2) IT IS A DEFENSE TO PROSECUTION UDER SUBSECTIONS (a)(2),
(b)(1(B), AND (b)(2)(B) THAT A DEFENDANT LACKED EDITORIAL CONTROL OVER THE
COMMUNICATIONS SPECIFIED IN THIS SECTION.

(3) IT IS A DEFENSE TO PROSECUTION UNDER SUBSECTIONS
(a)(2), (b)(1)(B), AND (b)(2)(B) THAT A DEFENDANT HAS TAKEN GOOD FAITH,
REASONABLE STEPS, AS APPROPRIATE --

(A) TO PROVIDE USERS WITH THE MEANS TO RESTRICT
ACCESS TO COMMUNICATIONS DESCRIBED IN THIS SECTION;

(B) PROVIDE USERS WITH WARNINGS CONCERNING THE
POTENTIAL FOR ACCESS TO SUCH COMMUNICATIONS;

(C) TO RESPOND TO COMPLAINTS FROM THOSE WHO ARE
SUBJECTED TO SUCH COMMUNICATIONS;

(D) TO PROVIDE MECHANISMS TO ENFORCE A PROVIDER'S
TERMS OF SERVICE GOVERNING SUCH COMMUNICATIONS; OR

(E) TO IMPLEMENT SUCH OTHER MEASURES AS THE
COMMISSION MAY PRESCRIBE TO CARRY OUT THE PURPOSES OF THIS
PARAGRAPH. NOTHING IN THIS SECTION IN AND OF ITSELF SHOULD BE CONSTRUED TO
TREAT ENHANCED INFORMATION SERVICES AS COMMON CARRIAGE.

(4) INADDITION TO OTHER DEFENSES AUTHORIZED UNDER THIS
SECTION, IT SHALL BE A DEFENSE TO PROSECUTION UNDER SECTION (b) THAT A
DEFENDANT IS NOT ENGAGED IN A COMMERCIAL ACTIVITY THAT HAS AS A PREDOMINATE
PURPOSE AN ACTIVITY
SPECIFIED IN THAT SUBSECTION.

(5) NO CAUSE OF ACTION MAY BE BROUGHT IN ANY COURT OR ANY
ADMINISTRATIVE AGENCY AGAINST ANY PERSON ON ACCOUNT OF ANY ACTION WHICH 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. THE PRECEDING SENTENCE SHALL NOT
APPLY WHERE THE GOOD FAITH DEFENSES UNDER SUBSECTION (c)(2) APPLY.

(6) NO STATE OR LOCAL GOVERNMENT MAY IMPOSE ANY LIABILITY IN CONNECTION
WITH A VIOLATION DESCRIBED IN SUBSECTION (a)(2), (b)(1)(B), (b)(2)(B) THAT IS
INCONSISTENT WITH THE TREATMENT OF THOSE VIOLATIONS UNDER THIS SECTION
PROVIDED, HOWEVER, THAT NOTHING 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 OBLIGATIONS ON THE PROVISION OF INTERSTATE SERVICES.

(e) FOR PURPOSES OF SUBSECTION (a) AND (b), THE TERM 'KNOWINGLY'
MEANS AN INTENTIONAL ACT WITH ACTUAL KNOWLEDGE OF THE SPECIFIC CONTENT OF THE COMMUNICATION SPECIFIED IN THIS SECTION TO ANOTHER PERSON.

ABOUT THE CENTER FOR DEMOCRACY AND TECHNOLOGY

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>

www/ftp/gopher archives are currently under construction, and should be up and running by the end of March.

###

POLICY POST

March 30, 1995
Number 7

CENTER FOR DEMOCRACY AND TECHNOLOGY

A briefing on public policy issues affecting civil liberties online
---
CDT POLICY POST 3/30/95 Number 7

CONTENTS: (1) Senator Leahy's Floor Statement Opposing Exon Bill
(2) About the Center For Democracy and Technology

The Center for Democracy and Technology is pleased to distribute this statement delivered by Senator Patrick Leahy (D-VT) on the floor of the Senate today. Leahy makes clear his opposition to the bill, explains that the Exon approach is the wrong way to regulate interactive media, and declares that the bill would threaten the free speech and privacy rights of all users of interactive services.

At the close of his statement, Senator Leahy calls on the Interactive Working Group (an ad hoc group of civil liberties and computer/telecommunications industry groups coordinated by CDT) to explore alternatives to the Exon bill. We are delighted to have such a strong civil liberties advocate on our side in the struggle over protecting and defining free speech in interactive media.

STATEMENT OF SENATOR LEAHY ON CENSORING CYBERSPACE

MARCH 30, 1995

Mr. President: I rise today to speak about legislation that would impose government regulation on the content of communications transmitted over computer networks. Ironically, this legislation was accepted without debate by the Commerce Committee as an amendment to a draft telecommunications bill whose purported purpose is to remove regulation from significant parts of the telecommunications industry. It is rumored that this matter could be headed for consideration by the Senate on Monday, although the bill has yet to be introduced and the Commerce Committee has yet to issue its report on the measure.

There is no question that we are now living through a revolution in telecommunications with cheaper, easier to use and faster ways to communicate electronically with people within our own homes and communities, and around the globe.

A byproduct of this technical revolution is that supervising our children takes on a new dimension of responsibility. Very young children are so adept with computers that they can sit at a keypad in front of a computer screen at home or at school and connect to the outside world through the Internet or some other on-line service. Many of us are, thus, justifiably concerned about the accessibility of obscene and indecent materials on-line and the ability of parents to monitor and control the materials to which their children are exposed. But government regulation of the content of all computer communications, even private communications, in violation of the First Amendment is not the answer-- it is merely a knee-jerk response.

Although well-intentioned, my good friend from Nebraska, Senator Exon, is championing an approach that I believe unnecessarily intrudes into personal privacy, restricts freedoms and upsets legitimate law enforcement needs. He successfully offered the Commerce Committee an amendment that would make it a felony to send certain kinds of communications over computer networks, even though some of these communications are otherwise constitutionally protected speech under the First Amendment. This amendment would chill free speech and the free flow of information over the Internet and computer networks, and undo important privacy protections for computer communications. At the same time, this amendment would undermine law enforcement's most important tool for policing cyberspace by prohibiting the use of court-authorized wiretaps for any "digital communications".

Under this Exon Amendment, those of us who are users of computer e-mail and other network systems would have to speak as if we were in Sunday School every time we went on-line. I, too, support raising our level of civility in communications in this country, but not with a government sanction and possible prison sentence when someone uses an expletive. The Exon amendment makes it a felony punishable by two years imprisonment to send a personal e-mail message to a friend with "obscene, lewd, lascivious, filthy, or indecent" words in it. This penalty adds new meaning to the adage, "Think twice before you speak." All users of Internet and other information services would have to clean up their language when they go on-line, whether or not they are communicating with children.

It would turn into criminals people, who in the privacy of their own homes, download racy fiction or "indecent" photographs. This would have a significant chilling effect on the free flow of communications over the Internet and other computer networks. Furthermore, banning the use of "lewd, filthy, lascivious or indecent words, which fall under constitutional protection, raises significant First Amendment problems.

Meanwhile, the amendment is crafted to protect the companies who provide us with service. They are given special defenses to avoid criminal

liability. Such defenses may unintentionally encourage conduct that is wrong and borders on the illegal.

For example, the amendment would exempt those who exercise no editorial control over content. This would have the perverse effect of stopping responsible electronic bulletin board system (BBS) operators from screening the boards for hate speech, obscenity and other offensive material. Since such screening is just the sort of editorial control that could land BBS operators in jail for two years if they happened to miss a bit of obscenity put up on a board, they will avoid it like the plague. Thus, this amendment stops responsible screening by BBS operators.

On the other hand, another defense rewards with complete immunity any service provider who goes snooping for smut through private messages. According to the language of the amendment, on-line providers who take steps "to restrict or prevent the transmission of, or access to" obscene, lewd, filthy, lascivious, or indecent communications are not only protected from criminal liability but also from any civil suit for invasion of privacy by a subscriber. We will thereby deputize and immunize others to eavesdrop on private communications. Overzealous service providers, in the guise of the smut police, could censor with impunity private e-mail messages or prevent a user from downloading material deemed "indecent" by the service provider.

I have worked hard over my years in the Senate to pass bipartisan legislation to increase the privacy protections for personal communcations over telephones and on computer networks. With the Exon amendment, I see how easily all that work can be undone -- without a hearing or even consideration by the Judiciary Committee, which has jurisdiction over criminal laws and constitutional matters such as rights of privacy and free speech.

Rather than invade the privacy of subscribers, one Vermonter told me he would simply stop offering any e-mail services or Internet access. The Physician's Computer Company in Essex Junction, Vermont, provides Internet access, e-mail services and medical record tracking services to pediatricians around the country. The President of this company let me know that if this amendment became law, he feared it would "cause us to lose a significant amount of business." We should be encouraging these new high-tech businesses, and not be imposing broad-brush criminal liability in ways that stifle business in this growth industry.

These efforts to regulate obscenity on interactive information services will only stifle the free flow of information and discourage the robust development of new information services. If users realize that to avoid criminal liability under this amendment, the information service provider is routinely accessing and checking their private communications for obscene, filthy or lewd language or photographs, they will avoid using the system.

I am also concerned that the Exon Amendment would totally undermine the legal authority for law enforcement to use court-authorized wiretaps, one of the most significant tools in law enforcement's arsenal for fighting

crime. The Exon Amendment would impose blanket prohibition on wiretapping "digital communications." No exceptions allowed.

This means that parents of a kidnapping victim could not agree to have the FBI listen in on calls with the kidnapper, if these calls were carried in a digital mode. Or, that the FBI could not get a court order to wiretap the future John Gotti, if his communications were digital. Many of us worked very hard over the last several years and, in particular, during the last Congress, with law enforcement and privacy advocates to craft a carefully balanced digital telephony law the increased privacy protections while allowing legitimate law enforcement wiretaps. That work will be undercut by the amendment. Our efforts to protect kids from on-line obscenity need not gut one of the most important tools the policy have to catch crooks, including on-line criminals, their ability to effectuate court-ordered wiretaps.

The problem of policing the Internet is complex and involves many important issues. We need to protect copyrighted materials from illegal copying. We need to protect privacy. And we need to help parents protect their children.

I have asked a coalition of industry and civil liberties groups, called the Interactive Working Group, to address the legal and technical issues for policing electronic interactive services. Instead of rushing to regulate the content of information services with the Exon amendment, we should encourage the development of technology that gives parents and other consumers the ability to control the information that can be accessed over a modem.

Empowering parents to control what their kids access over the Internet and enabling creators to protect their intellectual property from copyright infringement with technology under their control is far preferable to criminalizing users or deputizing information service providers as smut police.

Let's see what this coalition comes up with before we start imposing liability in ways that could severely damage electronic communications systems, sweep away important constitutional rights, and undercut law enforcement at the same time.

We should avoid quick fixes today that would interrupt and limit the rapid evolution of electronic information systems -- for the public benefit far exceeds the problems it invariably creates by the force of its momentum.

ABOUT THE CENTER FOR DEMOCRACY AND TECHNOLOGY

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>

www/ftp/gopher archives are currently under construction, and should be up and running by the end of March.

voice: 202.637.9800

###

POLICY POST

April 7, 1995
Number 8

CENTER FOR DEMOCRACY AND TECHNOLOGY

A briefing on public policy issues affecting civil liberties online
---
CDT POLICY POST 4/7/95 Number 8

CONTENTS: (1) Senator Leahy Introduces Alternative to Communications Decency Act
(2) Leahy Statement on Introdcution of S. 714
(3) Text of S. 714
(4) About the Center For Democracy and Technology

SUBJECT: Senator Leahy Introduces Alternative to Exon/Gorton Communications Decency Act

Senator Patrick Leahy (D-VT) today introduced the "Child Protection, User Empowerment, and Free Expression in Interactive Media Study Bill" (S. 714). The bill represents an alternative to Senator Exon (D-NE) and Senator Gorton's (R-WA) "Communications Decency Act", which would criminalize the transmission of any content deemed "obscene, indecent, lewd, lascivious, filthy, or harassing."

Leahy's bill would direct the Department of Justice, in consultation with the Commerce Department, to conduct a study to address technical means for empowering users to control information they receive over interactive communications systems such as the Internet, commercial online services, independent BBS's, and future interactive media. The bill is being co-sponsored by Senators Bob Kerry (D-NE) and Herb Kohl (D-WI), and is expected to generate support across party lines.

The Communications Decency Act, which Leahy seeks to replace, is now pending before the Senate as part of the "Telecommunications Competition and Deregulation Act of 1995' (S. 652).

In a statement announcing the introduction of the bill, Senator Leahy urged Congress to carefully consider the implications of imposing content restrictions on interactive media. "Heavy-handed efforts by government to regulate obscenity on interactive information services will only stifle the

free flow of information, discourage the robust development of new information services, and make users avoid using the system" Leahy said.

Instead, Leahy urged a careful consideration of possible alternatives before Congress attempts to legislate in this area. Under the legislation introduced today, the Department of Justice, in consultation with the Department of Commerce, would examine:

Whether current laws prohibiting the distribution of obscenity and child pornography by means of computers are sufficient.

Whether current law enforcement resources are sufficient to enforce existing laws.

The availability of technical means to enable parents and other users to control access to "commercial, non-commercial, violent, sexually explicit, harassing, offensive, or otherwise unwanted" content.

Recommendations to encourage the development and deployment of such technologies

The availability of technical means to promote the free flow of information consistent with Constitutional values.

The Center for Democracy and Technology commends Senator Leahy for his leadership on this issue and his efforts to promote the free flow of information in cyberspace. CDT will work to support Senator Leahy's efforts and to develop alternatives to content restrictions in interactive media.

LEAHY STATEMENT ON INTRODUCTION OF S. 714

STATEMENT OF SENATOR LEAHY
On Introduction of The Child Protection, User Empowerment, and Free Expression In Interactive Media Study Bill

April 7, 1995

Mr. President: I rise today to introduce a bill calling for a study by the Department of Justice, in consultation with the U.S. Department of Commerce on how we can empower parents and users of interactive telecommunications systems, such as the Internet, to control the material transmitted to them over those systems. We must find ways to do this that do not invite invasions of privacy, lead to censorship of private online communications, and undercut important constitutional protections.

Before legislating to impose government regulation on the content of communications in this enormously complex area, I feel we need more information from law enforcement and telecommunications experts. My bill calls for just such a fast-track study of this issue.

There is no question that we are now living through a revolution in telecommunications with cheaper, easier to use and faster ways to communicate electronically with people within our own homes and communities, and around the globe.

A byproduct of this technical revolution is that supervising our children takes on a new dimension of responsibility. Very young children are so adept with computers that they can sit at a keypad in front of a computer screen at home or at school and connect to the outside world through the Internet or some other on-line service. Many of us are, thus, justifiably concerned about the accessibility of obscene and indecent materials on-line and the ability of parents to monitor and control the materials to which their children are exposed. But government regulation of the content of all computer and telephone communications, even private communications, in violation of the First Amendment is not the answer -- it is merely a knee-jerk response.

Heavy-handed efforts by government to regulate obscenity on interactive information services will only stifle the free flow of information, discourage the robust development of new information services, and make users avoid using the system.

The problem of policing the Internet is complex and involves many important issues. We need to protect copyrighted materials from illegal copying. We need to protect privacy. And we need to help parents protect their children. Penalties imposed after the harm is done is not enough. We need to find technical means from stopping the harm done before it happens.

My bill calls for a study to address the legal and technical issues for empowering users to control the information they receive over electronic interactive services. Instead of rushing to regulate the content of information services, we should encourage the development of technology that gives parents and other consumers the ability to control the information that can be access over a modem.

Empowering parents to manage what their kids access over the Internet with technology under their control is far preferable to some of the bills pending in Congress that would criminalize users or deputize information service providers as smut police.

Let's see what this study reveals before we start legislating in ways that could severely damage electronic communications systems, sweep away important constitutional rights, and undercut law enforcement at the same time.

I ask unanimous consent, to have printed in the record at this pint, the "Child Protection, User Empowerment, and Free Expression in Interactive Media Study" bill.

TEXT OF S. 714

104th Congress
1st Session

S. 714

IN THE SENATE OF THE UNITED STATES

Mr. Leahy introduced the following bill; which was read twice and referred to the committee on_____

A BILL

To require the Attorney General to study and report to Congress on the means of controlling the flow of violent, sexually explicit, harassing, offense, or otherwise unwanted material in interactive telecommunications systems.

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

SECTION 1. STUDY ON MEANS OF RESTRICTING ACCESS TO UNWANTED MATERIAL IN INTERACTIVE TELECOMMUNICATIONS SYSTEMS.

(a) STUDY AND REPORT. -- Not later than 150 days after the date of enactment of this Act, the Attorney General shall complete a study and submit to the Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives a report containing --

(1) an evaluation of whether current criminal laws governing the distribution of obscenity over computer networks and the creation and distribution of child pornography by means of computers are fully enforceable in interactive media;

(2) an assessment of the Federal, State, and local law enforcement resources that are currently available to enforce those laws;

(3) an evaluation of the technical means available to --

(A) enable parents to exercise control over the information that their children receive and enable other users to exercise control over the commercial and noncommercial information that they receive over interactive telecommunications systems so that they may avoid violent, sexually explicit, harassing, offensive, or otherwise unwanted material; and

(B) promote the free flow of information consistent, with Constitutional values, in interactive media; and

(4) recommendations to encourage the development and deployment of technical means, including hardware and software, to enable parents to

exercise control over the information that their children receive and enable other users of exercise control over the information that they receive over interactive telecommunications systems so that they may avoid harassing, violent, sexually explicit, harassing, offensive, or otherwise unwanted material.

(b) CONSULTATION -- In conducting the study and preparing the report under subsection (a), the Attorney General shall consult with the National Telecommunications and Information Administration of the Department of Commerce.

ABOUT THE CENTER FOR DEMOCRACY AND TECHNOLOGY

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>

CDT's www site is up! Visit us at http://www.cdt.org/

Our ftp and gopher sites will be up soon.

voice: 202.637.9800

###

POLICY POST

April 11, 1995
Number 9

CENTER FOR DEMOCRACY AND TECHNOLOGY

A briefing on public policy issues affecting civil liberties online
---
CDT POLICY POST 4/11/95 Number 9

CONTENTS: (1) House CDA Sponsor Calls for Hearings, Go-Slow Approach
(2) Text of Rep. Tim Johnson's Letter to Chairman Fields
(3) About the Center For Democracy and Technology

SUBJECT: House CDA Sponsor Calls for Hearings, Go-Slow Approach

Representative Tim Johnson (D-SD) recently sent the attached letter to Rep. Jack Fields (R-TX), chairman of the House Subcommittee on Telecommunications and Finance, urging the subcommittee to carefully examine the issues raised by the legislation before rushing to enact it.

In the letter, Johnson clarifies that he sponsored HR 1004 only to facilitate a discussion and hearings on the issue. Johnson writes that while "it is essential for your committee to consider obscenity, harassment, and First Amendment concerns as well as over-all enforceability matters ... it is my hope that you will hold hearings which permit all points of view to be heard before taking any action on this issue."

The House Subcommittee on Telecommunications and Finance is currently drafting legislation to overhaul the Nation's telecommunications laws. A modified version of the Exon/Gorton "Communications Decency Act" (S. 314) was incorporated into similar legislation approved last month by the Senate Commerce Committee.

HR 1004 is the House counterpart to the Exon/Gorton Communications Decency Act, which would criminalize the transmission of any content deemed "obscene, indecent, lewd, lascivious, filthy, or harassing." Unlike the Senate version, HR 1004 has not been modified since its introduction.

CDT wishes to thank People for the American Way for obtaining a copy of this letter and forwarding it to us for distribution.

April 3, 1995

The Honorable Jack Fields
Chairman
Subcommittee on Telecommunications
and Finance
House Committee on Commerce
2125 Rayburn House Office Building
Washington, DC 20515

Dear Jack:

I am writing to you today relative to legislation which I have sponsored, HR 1004, a house counterpart to Senator Exon's S. 314, the Communications Decency Act. S. 314 was recently incorporated by voice vote into the Senate Commerce Committee's telecommunications reform legislation. The amendment attempts to update the Communications Act of 1934 by providing users of digital communications the same protections telephone users currently have against obscene, indecent, or harassing telephone calls.

I want to advise you that I have sponsored HR 1004 simply as a beginning point for hearings and discussion and not necessarily to propose that this bill, or any bill for that matter, is necessarily the proper response to concerns over obscenity. While it appears that the Exon provision as amended goes a long way to address the liability questions by exempting companies or entities which merely provide transmission services for the Internet, I remain concerned that this issue needs a thorough examination through the hearing process.

It is essential for your committee to consider obscenity, harassment, and First Amendment concerns as well as over-all enforceability matters. For that reason, it is my hope that you will hold hearings which will permit all points of view to be heard before taking any action on this issue. Hopefully, you and your committee will have an opportunity to consider this important issue in a carefully deliberative fashion which will balance concerns for children and others from unwanted obscene material on the Internet with free and enhanced use of the Internet. It may very well be that this balance is best achieved by voluntary means rather than by new legislation, but I will be appreciative of your willingness to carefully investigate this complex issue.

Thank you for your attention to this matter.

Sincerely,
{sig}
Tim Johnson

cc: Ed Markey
Ranking Minority Member
Subcommittee on Telecommunications and Finance

ABOUT THE CENTER FOR DEMOCRACY AND TECHNOLOGY

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>

CDT's www site is up! Visit us at http://www.cdt.org/

Our ftp and gopher sites will be up soon.

voice: +1.202.637.9800

###

POLICY POST

April 27, 1995
Number 10

CENTER FOR DEMOCRACY AND TECHNOLOGY

A briefing on public policy issues affecting civil liberties online
---
CDT POLICY POST 4/27/95 Number 10

CONTENTS: (1) Clinton Administration Announces Counter Terrorism Plan
(2) Outline of Clinton Administration Proposal
(3) Communications Decency Act Update
(4) About the Center for Democracy and Technology

SUBJECT: Clinton Administration Announces Outline of Counter Terrorism Initiative.

The Clinton Administration today unveiled an outline of administration proposals to combat foreign and domestic terrorism in the wake of the Oklahoma City bombing. The outline is attached below.

These proposals on their face raise obvious civil liberties concerns, including government interference with privacy, free speech, free association and Forth Amendment rights. CDT is waiting for the Administration to elaborate and provide concrete legislative proposals so that we can assess the full civil liberties ramifications.

This document is merely an outline, not specific legislation or executive order. The administration is expected to produce a more formal proposal in the coming weeks. These proposals are likely to supplement the Omnibus Counter-Terrorism Act of 1995 (S. 390, HR 896), which is currently pending before Congress.

CDT believes that there must be substantial open, public discussion of these proposals and thier potential implications before any action is taken.

We have set up the following URL's to provide information on the counter-terrorism issue. Updates will be made as soon as more information becomes available.

World-Wide-Web:

http://www.cdt.org/policy/terrorism/

ftp:

ftp://ftp.cdt.org/pub/cdt/policy/terrorism/

Clinton Administration Counter Terrorism Initiative

I. Actions Already Announced by the President

(1) Pass the Omnibus Counter-Terrorism Act of 1995

This bill would provide clear Federal criminal jurisdiction for any international terrorist attack that might occur in the United States; provide Federal criminal jurisdiction over terrorists who use the United States as the place from which to plan terrorist attacks overseas; provide a workable mechanism, utilizing United States District Judges appointed by the Chief Justice, to deport expeditiously alien terrorists without risking the disclosure of national security information or techniques; provide a new mechanism for preventing fundraising in the United States that supports international terrorist activities overseas; and would implement an international treaty requiring the insertion of a chemical agent into plastic explosives when manufactured to make them detectable.

(2) Provide more tools to federal law enforcement agencies fighting terrorism

AMEND THE FAIR CREDIT REPORTING ACT TO EASE ACCESS TO FINANCIAL AND CREDIT REPORTS IN ANTI-TERRORISM CASES. This legislation provides for disclosures by consumer reporting agencies to the FBI for counterintelligence and counterterrorism purposes. The FBI has no mechanism for obtaining credit reports for lead purposes in counterterrorism cases. These reports are available to used car dealers and other merchants. The FBI currently has authority under the Right to Financial Privacy Act of 1978 to obtain similar records pursuant to a "National Security Letter" signed by a high-ranking FBI official. the same procedures and safeguards would apply to credit records under this proposal.

AMEND FEDERAL LAW TO ADOPT, IN NATIONAL SECURITY CASES THE STANDARD CURRENTLY USED IN OBTAINING A "PEN REGISTER" IN A ROUTINE CRIMINAL CASE. This proposal would extend the relaxed standard for obtaining "pen registers" and "trap and trace" device orders which already exists in routine criminal cases, to national security cases. A "pen register" is a device which records the number dialed on a telephone. A "trap and trace" devices is similar to "Caller ID," providing law enforcement with the telephone number from which a call originates. Neither "pen registers" nor "trap and trace" devices permit law

enforcement to monitor actual conversations being conducted. the current, higher-than-regular standard impedes the ability of the FBI to obtain surveillance coverage of terrorists and spies.

PASS LEGISLATION TO REQUIRE HOTEL/MOTEL AND COMMON CARRIERS TO PROVIDE RECORDS NECESSARY FOR FIGHTING TERRORISM. This proposal would require hotel/motel and common carriers such as airlines and bus companies to provide records to the FBI pursuant to authorized national security requests just as they must do now for virtually all state and local law enforcement. The FBI must now rely on the voluntary assistance of motel, hotel, and other innkeepers or common carriers regarding records of terrorists who may have stayed at the establishment or used the common carrier. The FBI has found that, while some of these entities voluntarily provide such information, an increasing number refuse, absent a court order, a subpoena, or other legal protection. In a counterterrorism case being conducted pursuant to the Attorney General's guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations, there is no legal mechanism, e.g. subpoena, available to obtain these records.

FULLY FUND THE FBI'S "DIGITAL TELEPHONY" INITIATIVE TO ASSURE COURT AUTHORIZED LAW ENFORCEMENT ACCESS FOR ELECTRONIC SURVEILLANCE TO DIGITIZED COMMUNICATIONS. This proposal would appropriate funds to implement recent amendments to statutes governing secure telephone transmission (digital telephony). These amendments require telephone carriers to install and maintain sophisticated equipment which would permit law enforcement to continue to conduct legal electronic surveillance.

CREATE AND ALLOCATE FUNDS FOR A SPECIAL FBI COUNTERTERRORIST AND COUNTERINTELLIGENCE FUND. This proposal will fund costs associated cases which arise in connection with terrorism crises, including logistics and other support.

Create an interagency Domestic Counterterrorism Center headed by the FBI. This proposal will establish a partnership effort between the Justice Department, including the FBI, and other federal and state law enforcement authorities to coordinate efforts within the United States.

(3) CONDUCT TERRORISM THREAT ASSESSMENT OF EVERY FEDERAL FACILITY IN THE COUNTRY WITHIN THE NEXT 60 DAYS. The President has directed the Attorney General to conduct this assessment and report her recommendations in 60 days. The assessment has already begun.

(4) DIRECT GSA TO REPLACE THE FEDERAL BUILDING IN OKLAHOMA CITY.

(5) DIRECT THE FBI DIRECTOR, THE ATTORNEY GENERAL, AND THE NATIONAL SECURITY ADVISER TO PREPARE A PRESIDENTIAL DECISION DIRECTIVE AUTHORIZING ANY AND ALL FURTHER STEPS NECESSARY TO COMBAT FOREIGN AND DOMESTIC TERRORISM.

II. New Legislative Proposals

(1) INVESTIGATIONS

HIRE APPROXIMATELY 1000 NEW AGENTS, PROSECUTORS, AND OTHER FEDERAL LAW ENFORCEMENT AND SUPPORT PERSONNEL TO INVESTIGATE, DETER, AND PROSECUTE TERRORIST ACTIVITY.

PASS LEGISLATION TO REQUIRE, WITHIN 1 YEAR, THE INCLUSION OF TAGGANTS IN STANDARD EXPLOSIVE DEVICE RAW MATERIALS WHICH WILL PERMIT TRACING OF THE MATERIALS POST-EXPLOSION. This proposal would require the inclusion of microscopic particles in certain raw materials, thereby permitting law enforcement to trace the source of the explosive even after a device has been detonated.

REQUIRE THE BATF TO STUDY AND REPORT ON 1) THE TAGGING OF EXPLOSIVE MATERIALS FOR PURPOSES OF IDENTIFICATION AND DETECTION; 2) WHETHER COMMON CHEMICALS USED TO MANUFACTURE EXPLOSIVES CAN BE RENDERED INERT FOR USE IN EXPLOSIVES; AND 3) WHETHER CONTROLS CAN BE IMPOSED ON CERTAIN PRECURSOR CHEMICALS USED TO MANUFACTURE EXPLOSIVES. In light of recent bombing incidents, there is a need to develop technologies that will make it possible to detect concealed explosives. Additionally, if bombings do take place, a means of providing some clues is needed to lead investigators to those responsible for the explosion. Moreover, since explosives can be manufactured using common agricultural and household materials, it is important to determine whether such materials can be manufactured in a manner so that their use in explosives is unlikely. Finally, the study would determine whether any reasonable controls can be placed on precursor chemicals, e.g., ammonium nitrate, which have many legitimate uses.

AMEND THE POSSE COMITATUS ACT TO PERMIT MILITARY PARTICIPATION IN CRIME-FIGHTING INVOLVING WEAPONS OF MASS DESTRUCTION. This proposal would amend Federal Laws, which severely limit the role of the military in domestic law enforcement, to permit military participation in criminal cases involving chemical, biological, and other weapons of mass destruction; areas in which the military has specialized expertise.

AMEND THE ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1868 TO CONSTITUTIONALLY ENHANCE USE OF ELECTRONIC SURVEILLANCE TO FIGHT TERRORISM. This proposal would: permit any federal felony to be used as a basis for an electronic surveillance order; ease restrictions on the use, in American court proceedings, of information from electronic surveillance conducted by foreign governments; forbid suppression of electronic evidence unless law enforcement acted in bad faith in obtaining the evidence; authorize emergency electronic surveillance in situations involving threats by domestic terrorist organizations, authorize roving wiretaps where it is not practical to specify the number of the phone to be tapped, such as where a target uses multiple pay phones; allow the FBI to obtain records of local telephone calls, without the need for a court order, as they can own obtain records of long-diastase calls; and require telephone companies and/or service providers to preserve evidence until a court order could be obtained. None of these changes would alter the requirement for probable cause

prior to engaging in electronic surveillance.

(2) PROSECUTION

AMEND FEDERAL LAW TO CRIMINALIZE THE USE OF ALL CHEMICAL WEAPONS TO INCLUDE ALL FORMS OF CHEMICAL WEAPONS. This bill would amend federal law to include chemical weapons in non-gaseous form. Under existing law, chemical weapons in gaseous form are covered, but those which are in liquid or solid form are not. Thus, for example, an individual who introduces dioxin in solid form into the water supply of a city would not be chargeable under current law.

MAKE IT ILLEGAL TO POSSESS EXPLOSIVES KNOWING THAT THEY ARE STOLEN. This proposal would conform explosive laws to existing firearms statutes, making it a crime for an individual to possess explosives which the individual knows are stolen.

EXTEND THE STATUTE OF LIMITATIONS ON THE NATIONAL FIREARMS ACT TO FIVE (5) YEARS. This proposal would extend from three (3) to five (5) years the statute of limitations for prosecution for violations of the National Firearms Act, which deals with explosive and incendiary bombs. This change brings the statue of limitations for these offenses in line with similar criminal provisions.

PROVIDE THE SECRETARY OF TREASURY AUTHORITY TO DIRECT THE USE OF TREASURY DEPARTMENT AIRCRAFT TO SUPPORT EMERGENCY LAW ENFORCEMENT SITUATIONS. This proposal would authorize the Secretary of Treasury to authorize the use of Treasury Department aircraft in support of emergency law enforcement crises.

AMEND REWARD STATUTES TO REDUCE RESTRICTIONS ON MAKING REWARDS. This proposal would provide the Attorney General authority to pay a reward which is not subject to the spending limitations contained in 18 USC ¤¤ 3059 and 3072, provided that any reward of $100,000 or more may not be made without the approval of the President of the Attorney General, and such approval may not be delegated.

(3) PENALTIES

INCREASE THE PENALTY FOR ANYONE CONVICTED OF TRANSFERRING A FIREARM OR EXPLOSIVE KNOWING THAT IT WILL BE SUE DOT COMMIT A CRIME OF VIOLENCE OR DRUG TRAFFICKING CRIME. This proposal will provide a mandatory penalty of not less than 10 years for any person who transfers a firearm knowing or having reasonable cause to believe that a firearm will be used to commit a crime of violence or drug-trafficking crime.

AMEND 18 USC ¤ 111 TO PROVIDE ENHANCED PENALTIES FOR ALL CURRENT AND FORMER FEDERAL EMPLOYEES AGAINST TERRORIST ATTACKS. The existing statute only protects enumerated categories of current Federal employees. The proposed statute would provide enhanced penalties for crimes against all current and former Federal employees, and their immediate families, when the crime is committed because of the official duties of the federal employee.

UPDATE: Communications Decency Act Senate Vote Expected by June

The Senate is expected to consider telecommunications reform legislation (S. 652), which includes the Exon/Gorton Communications Decency Act (Title IV), sometime towards the end of May or begining of June. The vote had been expected to occur in the first week of May, but other issues, including counter-terrorism legislation, are likely to delay Senate action.

Senator Patrick Leahy's (D-VT) alternative proposal (S. 714) is gaining support among key members of congress and industry. CDT is working with Senator Leahy, the public interest community, and representatives of the communicaitons, computer, online services, and publishing industries to generate support for Senator Leahy's proposal.

Action on the House version of the CDA (HR 1004) is not expected to occur any time soon as its sponsor, Rep. Tim Johnson (D-SD) has recently backed away from the proposal. In a letter to Rep. Jack Fields (R-TX and Chair of the Hse. Telecomm. Subcommitte), circulated by CDT, Rep. Johnson urged the Committee to hold hearings and consider alternatives to protect children from controversial content instead of rushing to enact the CDA.

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

---

ABOUT THE CENTER FOR DEMOCRACY AND TECHNOLOGY

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/

gopher:

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

voice: +1.202.637.9800

###

POLICY POST

May 4, 1995
Number 11

CENTER FOR DEMOCRACY AND TECHNOLOGY

A briefing on public policy issues affecting civil liberties online
---
CDT POLICY POST 5/4/95 Number 11

CONTENTS: (1) Justice Department Says CDA Threatens First Amendment and Privacy Rights, Recommends Comprehensive Review
(2) Pro-Family Group says CDA is Flawed
(3) About the Center for Democracy and Technology

SUBJECT: Justice Department Says CDA Threatens First Amendment and Privacy Rights, Recommends Comprehensive Review.

The US Department of Justice, in a May 3, 1995 letter sent to Senator Patrick Leahy (D-VT), has weighed in on the debate over the Communications Decency Act, stating that it threatens first amendment and privacy rights and would severely complicate ongoing efforts to prosecute child pornography cases. The Department instead recommended a comprehensive review of current law and law enforcement resources, as well as an investigation into the availablity of technical means to empower parents and users to control the commercial and noncommercial content they receive through interactive media. The full text of the DOJ letter is available thru CDT's online archives (URL's below).

The Justice Department wrote:

"With respect to the communications Decency Act, while we understand that section 402 is intended to provide users of online services the same protection against obscene and harassing communications afforded to telephone subscribers, this provision would not accomplish that goal. Instead, it would significantly thwart enforcement of existing laws regarding obscenity and child pornography, create several ways for distributors and packages of obscenity and child pornography to avoid criminal liability, and threaten important First Amendment and privacy rights."

<...>

"Despite the flaws in these provisions, the Administration applauds the primary goal of this legislation: prevent obscenity from being widely transmitted over telecommunications networks to which minors have access. However, the legislation raises complex policy issues that merit close examination prior to Congressional action. We recommend that a comprehensive review be undertaken of current laws and law enforcement resources for prosecuting online obscenity and child pornography, and the technical means available to enable parents and users to control the commercial and non commercial communications they receive over interactive telecommunications systems."

In addition, the Department raised specific concerns regarding the constitutionality of the legislation:

"First, Section 402 of the bill would impose criminal sanctions on the transmission of constitutionally protected speech. Specifically, subsections 402(a)(1) and (b)(2) of the bill would criminalize the transmission of indecent communications, which are protected by the First Amendment. In _Sable Communications of Cal. v. FCC_, 492 U.S. 115 (1989), the Supreme Court ruled that any restrictions on the content of protected speech in media other than broadcast media must advance a compelling state interest and be accomplished by the "least restrictive means." By relying on technology relevant only to 900 number services, section 402 fails to take into account less restrictive alternatives utilizing existing and emerging technologies which enable parents and other adult users to control access to content."

"Nearly ten years of litigation, along with modifications of the regulations, were necessary before the current statute as applied to audiotext services, or "dial-a-porn" calling numbers, was upheld as constitutional. See _Dial Information Services v. Thornburg_, 938 F. 2d 1535 (2d Cir. 1991). The proposed amendment in section 40-2 of the bill would jeopardize the enforcement of the existing dial-a-porn statute by inviting additional constitutional challenges, with the concomitant diversion of law enforcement resources."

The Justice Department Letter represents an important development in the fight to block the Communications Decency Act and the effort to develop less restrictive technical alternatives. The Center For Democracy and Technology commends the Justice Department for recognizing the threat the Communications Decency Act poses to First Amendment rights and for its leadership in this area. CDT is looking forward to working with the Department to develop alternative prolicy solutions which protect the First Amendment, privacy rights, and the free flow of information in cyberspace.

The full text of the letter can be found at the following URL's:

http://www.cdt.org/speech/cda/950503doj_ltr.html

ftp://ftp.cdt.org/pub/cdt/policy/freespeech/doj_050395.ltr

---

(2) SUBJECT: American Family Association Expresses Concern about CDA, Says Defenses Must Be Axed, Current Law Sufficient.

The American Family Association, a conservative pro-family organization, has sent a letter to Senators Exon (D-NE) and Pressler (R-SD) stating that the Communications Decency Act as currently drafted would grant those who distribute pornography on the Internet greater protection than exists for current law. The American Family Assocaition reccomended that the defenses to prosecution be removed from the legislation.

The letter states that, in its current form, "...the pro-family movement will uniformly oppose your (Sen. Exon) bill and, if necessarry, the telecommunications bill to which it is attached, unless significant changes are made prior to a vote on the Senate floor."

The American Family Association stated that current law is sufficient to address the concerns Senator Exon is attempting to address:

"... it is unnecessary to change that law as your bill would do, unless you are seeking to clarify this point and add improvements to the law. Also, it is my opinion, although this point may not be as clear or settled as the first, that federal criminal law, s pecifically Title 18 Sections 1462 and 1465 prohibits distribution of obscenity via computer whether or not for commercial purpose. Further, it is my opinion that a primary problem regarding computer pornography is the lack of leadership and enforcement on this issue by the Clinton Administration. While current laws could be improved, the Administration could make substantial progress in protecting children in particular from both obscenity and child pornography by using existing law to prosecute illegal pornographers who use the Internet if it had the will to do so."

The American Family Association is the second pro-family group to publicly express concerns over the Communications Decency Act (in March Morality In Media raised similar concerns).

The full text of the American Family Association Letter, as well as the Morality In Media statement, can be found at the following URL's:

http://www.cdt.org/speech/cda/950404amfam_exon_ltr.html
http://www.cdt.org/speech/cda/950426amfam_pressler_ltr.html
http://www.cdt.org/speech/cda/950328mim_pr.html

ftp://ftp.cdt.org/policy/freespeech/amfam_exon.ltr
ftp://ftp.cdt.org/policy/freespeech/amfam_pressler.lt
ftp://ftp.cdt.org/policy/freespeech/mim_pr

---

(3) ABOUT THE CENTER FOR DEMOCRACY AND TECHNOLOGY

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

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.

voice: +1.202.637.9800

###

POLICY POST

May 8, 1995
Number 12

CENTER FOR DEMOCRACY AND TECHNOLOGY

A briefing on public policy issues affecting civil liberties online
---
CDT POLICY POST Number 12 May 8, 1995

CONTENTS: (1) FCC Modifies Caller ID Policy
(2) About the Center for Democracy and Technology

SUBJECT: FCC MODIFIES CALLER ID POLICY

On Thursday, May 4, 1995, the Federal Communications Commission voted to approve national Caller ID rules requiring carriers to provide "a free, simple and consistent, per call blocking and unblocking mechanism." In addition, under the new rules carriers are permitted to extend per-line blocking options selected by consumers for intrastate calls, to the consumers interstate calls. This action reverses an earlier rule adopted in March 1994, that required separate systems for intrastate and interstate calls. The Commissions earlier rules allowed for per-call blocking only. The new rules take effect December 1, 1995.

The Center for Democracy and Technology supports the new FCC policy on Caller ID. Caller ID or Automatic Number Identification (ANI) is a device that displays to a recipient of a call the telephone number of an incoming call while the phone is ringing.

The introduction of Caller ID technology sparked an emotional and divisive debate. The unlimited use of Caller ID threatened to place the privacy rights of the individual in his or her capacity as maker and receiver of telephone calls in tension. Civil liberties organizations were quick to point out that technology was available to honor the privacy right of the consumer in their capacity as both the sender and recipient of phone calls. Civil liberties organizations stated that through blocking users of telephones could be given control over information. For the caller, blocking allows them to choose when and to whom to release their phone number. For the recipient, blocking provides receivers with information that an incoming caller does not want their phone number revealed. Additional features can allow recipients of phone calls to

choose whether or not to refuse all incoming calls that employ blocking, send blocked calls to voice mail or answering machine, or exercise their option to answer or not answer the unidentified call on a per call basis.

The latest FCC policy responds to the dual civil liberty concerns of respecting and protecting the individual caller's privacy expectations, and respecting the important privacy interest of the receiver to limit intrusions by unknown, or unwanted callers.

THE NEW FCC POLICY:

1. Where a customer selects per-line blocking for in-state calls the new policy permits that choice to extend to interstate calls as well;

2. Permits customers to prohibit the transmission of Caller ID information - number, name, location - at all times, but on a per-call basis choose to release the information by using the code 82.

3. Binds states without Caller ID and blocking regulations to federal privacy protection models, which require per-calling blocking through the use of code 67.

CDT commends the FCC for issuing a policy that encourages technological development that maximizes individual choice and affirms individuals' expectations of privacy.

For More Information Contact:

Janlori Goldman, Deputy Director <jlg@cdt.org>
Deirdre Mulligan, Staff Counsel <deirdre@cdt.org>

---

(2) ABOUT THE CENTER FOR DEMOCRACY AND TECHNOLOGY

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>

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

May 12, 1995
Number 13

CENTER FOR DEMOCRACY AND TECHNOLOGY

A briefing on public policy issues affecting civil liberties online
---
CDT POLICY POST Number 13 May 12, 1995

CONTENTS: (1) CDT Testifies at Senate Judiciary Subcommittee Hearing On the Availability of Bomb-Making Materials on the Internet
(2) About the Center for Democracy and Technology

SUBJECT: CDT Testifies at Senate Judiciary Subcommittee Hearing On the Availability of Bomb-Making Materials on the Internet

The availability of bomb-making information and 'mayhem manuals' on the Internet was the subject of a hearing yesterday (5/11/95) before the Senate Judiciary Committee Subcommittee on Terrorism, Technology, and Government Information. CDT Executive Director Jerry Berman testified before the panel. Berman's testimony is available on CDT's online archives (URL's below).

The bombing in Oklahoma City has brought the Internet under new scrutiny by Congress and the Clinton Administration. In his opening statement, Subcommittee Chair Arlen Spector (R-PA) made clear the First Amendment issues raised by government efforts to censor certain material in cyberspace. However, Spector acknowledged that the availability of so called "mayhem manuals" (one of which he displayed before the hearing) raises concerns about public safety and national security.

Senator Patrick Leahy (D-VT), in his opening statement, urged caution and careful consideration of the benefits new communications technologies can bring before Congress rushes to restrict and limit its use.

"Before we head down a road that leads to censorship, we must think long and hard about its consequences. The same First Amendment that protects each of us and our right to think and speak as we choose, protects these

others as well. The rule of this free society has long been that it is harmful and dangerous conduct, not speech, that justify adverse legal consequences", Leahy said.

Senator Leahy, an opponent of Senator Exon's Communications Decency Act (S. 314), and strong advocate of freedom of speech and the free flow of information in cyberspace, recently introduced S. 714, an alternative to Senator Exon's bill (the text of Leahy's bill is available from CDT, URL below).

Witnesses on the panel included:

Jerry Berman, Executive Director, Center For Democracy and Technology
Rabbi Marvin Hier, Dean of the Simon Wiesenthal Center
Robert Litt, Deputy Assistant Attorney General, US Detp. of Justice
William Burrington, Assistant General Counsel. America Online
Prof. Frank Tuerkheimer, U. of Wisconsin Law School

What Does It Mean To "Shout Fire In Cyberspace?"

CDT's Jerry Berman acknowledged the availability of bomb-making instructions and terrorist manuals on the Internet, but argued that such materials deserve the same degree of protection as identical materials available in bookstores or libraries.

"As an open society, governed by the democratic principles of the First and Fourth Amendments, we tolerate and even encourage robust debate, advocacy and exchange of information on all subjects and in all media of expression, without exception. Prior restraint or any government action which might chill speech have long been labeled intolerable, expect in the few circumstances in which that speech advocates imminent violence and is likely to produce such violence. Even in these cases, Constitutional law and long-standing law enforcement policy have dictated great restraint in order to avoid chilling legitimate speech activity."

"Justice Holmes taught that the First Amendment does not protect a person from punishment for "falsely shouting fire in a theater and causing a panic," Schenk v. United States, 249 U.S. 47, 52 (1919), but what does it mean to "shout fire" in cyberspace? We believe that shouting fire in cyberspace is actually far less threatening, and thus less deserving of censure, than the equivalent act in the physical world. Though one can shout fire in an email message or on an Internet newsgroup, the likelihood that it will incite readers to imminent, criminal action is much reduced because the readers are dispersed around the country, and even around the world."

Berman added,

"The Center for Democracy and Technology believes that any prosecutorial or investigative activity must be predicated on speech plus a

reasonable indication that the speech will lead to imminent violence. Speech alone is not enough to prosecute or investigate in other media, and it should not be sufficient in interactive media. Moreover, we assert that current law and the FBI's strict interpretation of the existing Attorney General investigative guidelines are adequate to serve both law enforcement purposes and First Amendment interests.

In the sharpest exchange of the hearing, Senator Dianne Feinstein (D-CA), expressed strong concern about the ability of children to access bomb-making material on the Internet. Visibly outraged by the testimony, Feinstein said, "I have a problem with people who use the First Amendment to teach others how to kill [other people]" Protecting such speech, "... is not what this country is about."

CDT's Jerry Berman responded, "Excuse me, Senator, but that is what this nation is all about."

Feinstein countered that she believes that there is a " difference between free speech and teaching someone how to kill others", and suggested that the government should take a greater role in preventing the availability of such materials.

Deputy Assistant Attorney General Robert Litt, agreeing with CDT's assertion that the First Amendment protects bomb-making manuals and other such material regardless of the medium of distribution, added that the Justice Department has the authority under current law to prosecute individuals who use the Internet to commit crimes relating to "extortion, threats, conspiracy, and aiding and abetting the violation of other federal laws". But Litt emphasized that such prosecutions must be predicated by conduct.

Litt said:

"We can, therefore, clearly act to punish conduct that falls within the scope of existing laws. But when we address not conduct but possibly protected speech, the power of law enforcement is restricted by the First Amendment. As the Committee well knows, we must guard the public's right to free speech even while protecting the public from criminal activity. The Constitution imposes stringent limits on our ability to punish the mere advocacy of principals or the mere dissemination of information, without more, even if the communications in question are utterly repugnant".

However, the Justice Department staked out a more aggressive line on the issues of encryption and anonymity. On anonymity, Litt acknowledged the necessity of confidentiality for whistle-blowers and informants, but argued that the availability of complete anonymity on the Internet is of serious concern to law enforcement.

In his prepared testimony, Litt echoed FBI Director Louis Freeh's recent comments that "... unless the encryption issue is adequately addressed, criminal communications over the telephone and the Internet will be will be encrypted and inaccessible to law enforcement even if a court has

approved electronic surveillance," and pledged to continue to work to find solutions to this issue.

In a statement which appears to dredge up previous arguments from the Department in support of the Clipper Chip government key escrow proposal, Litt said:

"We believe that it is possible to deal with both of these issues -- encryption and anonymity. Privacy rights should generally be protected, but society should continue to have, under appropriate safeguards and when necessary for law enforcement, the ability to identify people and hold them accountable for their conduct. In the case of encryption, the appropriate balance can be achieved by the widespread use of reliable, strong cryptography that allows for government access, with appropriate restrictions, in criminal investigations and for national security purposes. The federal escrowed encryption standard issued last year is designed to achieve this delicate balance for voice telephony."

Rabbi Marvin Hier of the Simon Wiesenthal Center, argued that the nature of the Internet, including its broad reach and the veil of anonymity, provides a fertile ground for hate-groups and other potentially dangerous organizations. While stressing the importance of the First Amendment, Hier recommended that:

Law enforcement should have the ability to monitor hate groups and other organizations that clearly advocate an intention to commit violence that use the Internet to distribute information;

Online service providers (particularly the commercial services such as AOL and Compuserve) should take steps to prevent their networks from being used to distribute material from these organizations; and

To look at the uses of these communications technologies and to examine what legal limits can be placed on it.

William Burrington, Assistant General Counsel and Director of Government Affairs for America Online, stressed that AOL does take steps to address violations of its terms of service agreement, and has removed users who use the network to post inappropriate material to public forums.

However, Burrington cautioned that it is impossible and illegal under ECPA for a service provider to monitor every communication that travels across their network. Burrington further noted that, while it is possible for America Online to exercise limited control inside its own networks, monitoring and controlling content on the Internet is beyond the reach of any one because of the decentralized nature and global reach of the network.

Speaking from direct experience, University of Wisconsin Law Professor Frank Tuerkheimer stressed that the government should not attempt too prevent or censor the publication of bomb-making manuals or other such

materials -- not only because such action is clearly contrary to the First Amendment, but also because the material would inevitably be published in another forum, rendering the government's argument moot.

This is precisely what occurred in 1979 in United States v. Progressive, Inc (476 F. Supp 990 (W.D. Wisc. 1979). In this case, the government, sought to prevent the publication of instructions on how to make a hydrogen bomb. Professor Tuerkheimer was the federal prosecutor in the Progressive Case. The article was ultimately published and the case became moot because the information was found to be available in a number of public libraries.

Tuerkheimer noted that it would be futile for the government to attempt to prosecute someone for distributing bomb making material on the Internet, since information on how to build an ammonium nitrate bomb similar to the device used in the Oklahoma City tragedy can be found in encyclopedias and in publications available from the US Department of Agriculture.

NEXT STEPS:

Although the issue of the availability of bomb-making manuals and the use of the Internet by malitia and hate-groups has received considerable attention in the press and on Capitol hill in recent weeks, as of this writing there has been no legislation introduced, and so far none of the counter-terrorism proposals specifically address this issue.

CDT will closely track this issue, and will alert you to any developments as soon as they become available.

Paths to Relevant Documents

CDT Executive Director Jerry Berman's testimony is available at the following URL's:

http://www.cdt.org/policy/terrorism/internet_bomb.test.html

ftp://ftp.cdt.org/pub/cdt/policy/terrorism/internet_bomb.test

Additional hearing documents, including the Department of Justice testimony can be found at the following URL's

http://www.cdt.org/policy/terrorism/May11_hearing.html

<a href =

"ftp://ftp.cdt.org/pub/cdt/policy/terrorism/00-INDEX.terrorism">ftp://ftp.cdt.org/pub/cdt/policy/terrorism/00-INDEX.terrorism

The Text of S. 714, Senator Leahy's Alternative to the Communications Decency Act, can be found at:

<a href =
"/speech/cda/950407s714.html">http://www.cdt.org/speech/cda/950407s714.html

ftp://ftp.cdt.org/policy/legislation/s714.bill

---

(2) ABOUT THE CENTER FOR DEMOCRACY AND TECHNOLOGY

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>

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

May 26, 1995
Number 14

CENTER FOR DEMOCRACY AND TECHNOLOGY

A briefing on public policy issues affecting civil liberties online
---
CDT POLICY POST Number 14 May 26, 1995

CONTENTS: (1) Analysis of Proposed revision of Exon CDA By CDT and People For The American Way -- Bill Still Unconstitutional
(2) Text of Draft Revision
(3) Sign the Petition To Help Senator Leahy Fight the CDA
(4) Petition Update -- 10,000 sigs as of Friday 5/26/95!
(5) About CDT/Contacting Us

---
(1) SUBJECT: New Draft proposed to Revise Exon CDA -- Bill Still Unconstitutional

The Communications Decency Act, authored by Senator James Exon (D-NE), has attracted a firestorm of criticism from nearly all groups that are concerned about censorship, children's access to controversial material and the health of the Internet marketplace. Critics include the American Family Association, American Online, People for the American Way, and the United States Justice Department, as well as a variety of civil liberties and press groups. In an effort to seek a compromise among these disparate groups, some parties have drafted a legislative proposal as an alternative to the current Exon language in the Senate Telecommunications Reform bill. As far as we know, this draft has not yet been accepted by any parties.

We believe that the draft contains several significant improvements over the original language, but it still contains unconstitutional prohibitions against First Amendment-protected speech and fails to fully account for the unique characteristics of interactive media.

The Free Speech Rubicon for Interactive Media

The key flaw remaining in this proposal is its well-intentioned but overbroad effort to regulate indecent material (the "seven dirty words") in interactive media. Regulation of indecency has been found constitutional only in limited cases involving radio and television broadcasting and audiotext services. We believe that given the unique user control

attributes of interactive media, as well as the great abundance of capacity, it is unconstitutional to regulate indecency in this new medium. The result of this overbroad regulation is the paradoxical result that information which is freely available in bookstores, libraries and record shops will be barred on the Internet. Such restrictions will stifle the free flow of information in interactive media and deal a grave blow to the development of markets for multimedia products and services.

Based on our initial analysis, we have the following comments on the new language:

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.

Prohibited items under the new subsection (e) include:

Rap music lyrics (both the text and the sound files)
Lady Chatterly's Lover
Public eclaration that you're "pissed off" or that someone is a "shit."
Calvin Klein ads (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 regulate obscenity, but can only regulate indecency in very narrow circumstances, such as in the broadcast media where there is a captive audience. Even in these narrow circumstances, such regulation may be the "least intrusive means" for accomplishing the government's goal of protecting children. 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.

Furthermore, the government may not regulation indecent material in a way that would deny adults access to such material. 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.

B. 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.

C. 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.

Conclusion

In light of the serious constitutional concerns raised about the Act, and the danger that it poses for the development of a vital new communications medium, we believe that it is essential that the Congress given careful scrutiny and study to provisions involving the regulation of indecency in interactive media. Senator Leahy and Rep. Klink have offered legislation (S. 714) which would conduct just such as study. Thoughtful consideration is essential before moving ahead with legislation that is both unconstitutional and patently ineffective toward the goal of protecting children.

For more information contact:

Center for Democracy and Technology 202-637-9800
Jerry Berman <jberman@cdt.org>

Daniel Weitzner <djw@cdt.org>

People for the American Way 202-467-4999
Leslie Harris <laharris@tmn.com>
Jill Lesser <jlessern@counsel.com>

For background on the Communications Decency Act, see the Center for Democracy and Technology's World Wide Web site at http://www.cdt.org/.

---

(2) Proposed revision to Communications Decency Act
May 19, 1995 draft

NOTE: Changes indicated in this draft (as marked below) represent changes to the draft itself, and not to the language of the current Communications Decency Act (Title IV of S. 652). This draft would replace Title IV in its entirety.

[ ] = Deletion
text = Addition

Sec. 223. Obscene or harassing utilization of telecommunications devices and facilities in the District of Columbia or in interstate or foreign communications .

(a) Whoever --

(1) in the District of Columbia or in interstate or foreign communications by means of telecommunications device

(A) 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 communications 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 [and willfully] permits any telecommunications facility under his control to be used for any _activity_[purpose] prohibited by this subsection with the intent that it be [so] used _for such activity_.

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

NO CHANGES TO CURRENT LAW FOR SEC. (b) & (c)
"DIAL-A-PORN" Statute.

NEW SECTION (d)

(d) Whoever--

(1) knowingly within the United States by means of telecommunications device

(A) makes, creates, _or_ solicits, and
(B) initiates the transmission of or purposefully makes available

any comment, request, suggestion, proposal, image, or other communication which is obscene, regardless of whether the maker of such communication placed the call or initiated the communications, or

(2) knowingly [and willfully] permits any telecommunications facility under such person's control be used for an activity prohibited by subparagraph (d)(1) with the intent that it be so 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 by means of telecommunications device
(A) makes, creates, [or] solicits, and
(B)initiates the transmission of, or purposely makes available,

any indecent comment, request, suggestion, proposal, image, or other communication [which is available] to any person under 18 years of age [or to any person 18 years of age or older without that person's consent,] regardless of whether the maker of such communication placed the call or initiated the communications, or

(2) knowingly [and willfully] permits any telecommunications facility under such person's control be used for an activity prohibited by subparagraph (e)(1) with the intent that it will be so 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)[(2)], (d), and (e) restrictions on access, judicial remedies respecting restrictions for persons providing carriage or information services --

(1) _The provision of access by a_ person [including] transmission, downloading, storage, or navigational tools, and related capabilities which are incidental to the transmission of communications, and not involving the creation or alteration of the content of the communications), for another person's communications to or from a service, facility, system, or network not under _the access provider's_[that first person's] control _shall by itself not be a violation of subsection (a), (d) or (e)_. [This defense shall not be available to a defendant who is owned or controlled by or a conspirator with an entity actively involved in the creation, alteration or knowing distribution of communications which violate this section or to an entity which exists for the creation, alteration, or knowing distribution of communications which violate this section.]

(2) It is a defense to prosecution under subsections (a)(2), (d)(2) or (e)(2) that a defendant _did not have editorial contgrol_ over the [lacked the capability of exercising editorial control over the] communication specified in this section. This defense shall not be available to a defendant who has ceded editorial control to an entity which the defendant knows or [has substantial] _had_ reason to know intends to engage in conduct that is likely to violate this section.

(3) It is a defense to prosecution under subsections (a), (d)(2) and (e) that a defendant has taken good faith, reasonable steps, to restrict or prevent the transmission of, or access to communications described in [this section] _such provisions_ according to such procedures as the Commission may prescribe by regulation. _Such steps and FCC procedures may include enabling the user to restrict or prevent access to communication described in this section_. Nothing in this subsection [in and of itself] shall be construed to treat enhanced information services as common carriage.

(4) No cause of action may be brought in any court or administrate agency against any person on account of any [otherwise lawful] action _not in violation of any law punishable by criminal penalty_ which 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 a violation described in subsection (a)(2), (d)(2), or (e)(2) that is inconsistent with the treatment of those violations under this section provided, however, that nothing 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 obligations on the provision of interstate services. Furthermore, nothing in this subsection shall preclude any State or local government from governing conduct not covered by this section.

(h) Nothing in this subsection (a), (d) or (e) 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.

(3 & 4) PETITION UPDATE: 10,000 Signatures in the first week!

The petition in support of Senator Patrick Leahy's (D-VT) alternative to the Communication Decency Act has in its first week generated 10,000 signatures. Thank you to those of you who have already singed! With your help, we are
demonstrating that the net.community is a political force to be reckoned with.

If you have not signed the petition yet:

Visit the petition web page: http://www.cdt.org/petition.html

For instructions on how to sign via email (for thouse w/o access to the web):

send email to vtw@vtw.org with a subject send petition

---

(5) ABOUT THE CENTER FOR DEMOCRACY AND TECHNOLOGY

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

May 31, 1995
Number 15

CENTER FOR DEMOCRACY AND TECHNOLOGY

A briefing on public policy issues affecting civil liberties online
---
CDT POLICY POST Number 15 May 31, 1995

CONTENTS: (1) Senate Proposals Will Create National Identification System
(2) Letter from Right-Left Coalition Members Opposing National ID System.
(3) Status of and Paths to Relevant Documents
(4) About The Center For Democracy and Technology/Contacting Us

---

SUBJECT: SENATE PROPOSALS WILL CREATE A NATIONAL IDENTIFICATION SYSTEM

The Senate is currently considering proposals to create a national database containing personally identifiable information on every individual in America. Recommendations to create a national "worker verification" data system are central components of 3 bills currently before the Subcommittee on Immigration of the Judiciary Committee: S. 269, "The Immigrant Control and Financial Responsibility Act of 1995," introduced on January 24, 1995, by Senator Simpson (R-WY), Chairman of the Subcommittee, is scheduled for mark-up on June 6th; S. 580, the "Illegal Immigration Control and Enforcement Act of 1995," introduced on March 21, 1995, by Senator Feinstein; and, S. 754, the "Immigration Enforcement Improvements Act of 1995," introduced on May 1, 1995, by Senators Kennedy, Simon and Boxer.

The Center for Democracy and Technology is opposed to the creation of a computerized system to verify work eligibility. Such a system poses a substantial threat to privacy and is unlikely to accomplish the goal of eliminating the job market for undocumented immigrants.

Leading the opposition to the national identification system proposals is a coalition of organizations and individuals, including conservative/free market groups, representatives of the business community, civil rights organizations and civil liberties organizations.

The loudest protest against the pending bills has been voiced by the conservative and libertarian communities.

In a speech at the Cato Institute, House Majority Leader Dick Armey stated, "I will fight it. . .Any system in which Americans would be forced to possess such a card, for any reason, is an abomination and wholly at odds with the American tradition of individual freedom."

The Center for Equal Opportunity and the Alexis de Tocqueville Institute are leading the conservative/libertarian outcry. Stuart Anderson, Policy Director at the Alexis de Tocqueville Institute spoke out against the proposals in a recent Washington Times editorial, "The federal government has never before held detailed information on all Americans in one consolidated place accessible to government officials and outside entities. . . The IRS, Bureau of Alcohol Tobacco and Firearms, computer hackers, even private organizations such as banks, could potentially access a national computer database."

IN AN ATTEMPT TO ADDRESS THE PROBLEM OF UNDOCUMENTED WORKERS, ESTIMATED TO COMPRISE 1.5% OF THE TOTAL POPULATION, THE PROPOSALS CAST A BUREAUCRATIC NET AROUND 100% OF THE UNITED STATES POPULATION.

The coalition questions the logic of imposing a multi-billion dollar system of increased government bureaucracy upon the daily lives of Americans, at a time when less federal power and intrusion is the mantra of the day. As Anderson says, "The price of fake documents and acceptable Social Security numbers will likely increase, but there is no reason to believe the number of illegal immigrants working here will decrease." In this ill-conceived effort to address the problem of undocumented workers, every American worker will be forced to participate in an intrusive government system. This is truly an Orwellian nightmare.

Under the guise of reforming immigration policy the bills sponsors are asking Congress to authorize the creation of a broad worker verification registry that by design must contain information not just on illegal immigrants, but on every American and legal immigrant who desires to work. For the first time the federal government has created a detailed system of records on individuals that it intends to make accessible to the public. Rather than designing an effective system to manage immigration, these bills propose a national database that tramples on the civil rights and liberties of every American citizen and resident by subjecting each to unwanted and unnecessary invasions of privacy.

A NATIONAL WORKER VERIFICATION SYSTEM WILL NOT ACCOMPLISH ITS GOAL -- ELIMINATING THE JOB MARKET FOR UNDOCUMENTED IMMIGRANTS -- BUT IT WILL INCREASE DISCRIMINATION.

A worker verification system is an ineffective tool for curbing the job market for unauthorized workers, and is very likely to lead to increased discrimination and erode individual privacy. No matter what system or card is developed, the black market will continue to meet the demand for false documents. Employers who hire undocumented workers will continue

to violate the law; they do so intentionally and are unlikely to use a verification system. Instead they will continue to hire undocumented workers, while law-abiding employers are subject to new and costly government regulation. During the pilot study of the Telephone Verification System the projected costs to employers, for equipment and administration, ran between $1,075.00 and $16,155.

THE PROPOSALS WILL LEAD TO THE CREATION OF AN ALL PURPOSE NATIONAL IDENTITY DOCUMENT.

In a "Roll Call" article on May 22, 1995, Senator Feinstein made her preference for a single fraud-resistant document clear. Feinstein stated, "I believe that a new, phone or machine-readable card that all job and benefits applicants would be required to present . . . deserves careful consideration. . . counterfeit-resistant cards that incorporate 'biometric' data are available and in use today . . . whether the card carries a magnetic strip on which the bearer's unique voice, retina pattern, or fingerprint is digitally encoded. . . it is clear to me that state-of-the-art . . . IDs can and must replace the dinosaur age documents now being used." Although the Senate proposals do not call for the creation of a document to verify identity, the very design of a vast system of information makes the development of such a document inevitable. At a hearing held by the Subcommittee on Immigration on May 10, 1995, "Verification of Applicant Identity for Purposes of Employment and Public Assistance," it was quite clear that the creation of a national identity document is at the core of the "worker verification system" proposals.

The proposals will expand the treasure trove of information accessible to the unscrupulous individual who gets hold of another's SSN. The use of the SSN as the "worker verification identifier" will facilitate linkage between various systems of governmental and private sector records, making the inevitable temptation to use the data base for other purposes even stronger.

The proliferation of the Social Security Number, a number that by law was to be used exclusively within the social security system, offers a telling example of the Government's inability and unwillingness to limit the uses to which such a massive system of identification and tracking can be put. The SSN was created for a limited purpose. Over the past fifty years its use by both the government and private sector has proliferated. The SSN has become a multi-use identifier that can be used to link information contained in public and private sector databases. The SSN is a key that unlocks vast storehouses of information collected on American citizens, such as credit, health, driving and banking records.

AMERICANS WILL BE WRONGLY DENIED JOBS DUE TO INACCURATE DATA. According to a recent GAO report, over 65 million American's change jobs or enter the workforce each year. Even if the system's error rate was reduced to 1% over 650,000 people would inaccurately be denied the right to work each year due to faulty data. Each Americans' ability to work will be dependent on the accuracy of data from the Social Security

Administration and Immigration and Naturalization Service, both of which have been widely criticized for keeping inaccurate records. The INS recently admitted to losing 60,000 files of green-card applicants in California and is currently being sued by the American Civil Liberties Union. Current estimates reveal error rates in INS records as high as 30%. The Commissioner of Social Security, testifying in 1991 stated, "over 60 percent (of the SSNs in use today) are based on the assertions a person made at the time he or she applied for a SSN." According to the testimony of Gilbert Fisher, Assistant Deputy Commissioner of SSA before the Subcommittee on May 10th, the cost of reissuing the 270 million cards necessary to address the problem of cards issued without proof of identity would cost between 3 and 6 billion dollars.

In fact, during a recent hearing it became apparent that a bottom line figure for the accuracy level to be reached prior to deploying the "worker verification system" has not been established or seriously considered. It seems that the supporters of the bills would move forward on the "worker verification system" with full knowledge that individuals will be unfairly denied employment and benefits due to inaccurate data. Senator Feinstein seems to be the least concerned with the loss of employment and benefits by eligible individuals. In a Roll Call article on May 22, 1995, Senator Feinstein advocated moving forward immediately without the "pilot" studies and information gathering included in the majority of proposals.

A WORKER REGISTRY WILL BE ABUSED TO DISCRIMINATE AND INVADE PRIVACY.

The ability of the SSA or other government agency to monitor and control access to and use of an information system that is available to both agency employees and all potential employers is dubious. A "worker verification system" or national identity document is prone to abuse by persons who use it to selectively screen individuals whose appearance, surname or accent suggests they are foreign, or to screen such persons outside the employment context. The system or document will place a powerful weapon in the hands of those seeking to harass and discriminate.

In addition to unauthorized outside use of the system, the creation of a worker verification data system will subject individuals to invasions of privacy and discrimination from agency employees. Both the IRS and the SSA have recently been subject to criticism for their lack of control over agency employees who were both browsing through information for their own purposes, and making information available to outsiders for monetary compensation. The openness of the proposed worker verification system will make it more difficult to monitor and control the use of sensitive personal information and therefore subject individuals to greater invasions of personal privacy and discrimination from system misuse.

ANALYSIS OF SELECT SECTIONS OF BILLS:

1. The bills propose to expand the existing Telephone Verification

System (TVS) pilot

The TVS pilot project should not be expanded. During phase I, nine companies participated in a pilot to test the TVS project. This pilot has allowed companies to call the INS and ask for verification that non-citizens applying for work are eligible for employment. Both S. 269 and S. 754 call for an expansion of TVS.

Numerous flaws were illuminated during phase I of the TVS pilot which counsel strongly against its expansion and undermine its utility. First, it relies on "self- attestation" -- those presenting for employment must self identify as aliens -- to trigger the system. Illegal immigrants can avoid the pilot and never have their eligibility to work checked by simply claiming to be a citizen. Second, during the initial pilot, the INS found it was unable to make a determination of employment eligibility based on information contained in its computerized files 28% of the time, thus the INS had to perform a manual search to fulfill 28% of the verification requests.

2. S. 754 and S. 269 both recommend additional pilots that will improve, utilize and link the Social Security Administration (SSA) and Immigration and Naturalization Service (INS) records and data systems

S. 754 recommends the establishment of additional pilot projects that may include: a process which allows employers to verify the eligibility for employment of new employees using the SSA's records and if necessary, to conduct a cross-check using INS records; a simulated linkage of the electronic records of the INS and the SSA; and, improvements and additions to the electronic records of the INS and the SSA for the purpose of using such records for verification of employment eligibility. (Section 202) S. 269 directs the Administration to conduct demonstration projects in five states to test the feasibility of the system. (Section 112 (a),(b))

More importantly, Section 113 of S. 269 directs the Attorney General to establish a database containing information obtained from the Social Security Administration and the Immigration and Naturalization Service to be used in determining work authorization for individuals living in the United States within one year. The database may be used in conjunction with both the demonstration projects and the final system. This new data system will be managed by a new Office of Employment and Public Assistance Eligibility Verification.

The information collected by the Social Security Administration is insufficient for establishing identity. The creation of a national identification system run by the SSA, INS or a new agency would require a vast increase in data collection on individuals. For a system to accurately establish the identity of individuals it would need to contain information as to their identity - name, birth date and location, height and weight, for example - citizenship status, and most likely a biometric identifier, such as a fingerprint. Such a system would provide the government and private institutions with the ability to track and profile people from birth to death, creating what Professor

Arthur Miller termed a "womb-to-tomb" dossier.

Linking information contained in separate databases raises privacy concerns. By allowing government agencies to share information we accelerate the creation of a system of national identification, and condone the use of information individuals provided to the government with the understanding that it would be used for a limited purpose for additional purposes without the individual's consent.

Use of the Social Security Number (SSN) and the underlying SSA database to verify the eligibility of individuals to work is impracticable and threatens privacy. Like the INS database, the SSA database is riddled with errors. The SSN was never intended to be relied on by itself as foolproof identification. Historically, SSNs have been easy to obtain because there was no need for a secure card for Social Security Administration purposes.

Even with the strictest security measures it is impossible to build an impenetrable system. The database will be a target for computer hackers who want information on individuals. Although both S. 269 and 2. 745 contain provisions regarding use and protection of the data, the ability of the federal government to limit the use of large databases by the government and private sector is doubtful.

The "pilot" programs and "worker verification" system proposed by these bills are a huge step toward the establishment of a system of national identification and the creation of a national identification document. The designation of the projects as "pilots" is misleading. Under the guise of limited "pilot" projects the government is building the basic infrastructure necessary to implement a wholesale worker verification system. The language used in the proposals masks the cold fact that actual individuals will be denied jobs and benefits, during the "test" of these "pilots." A significant number of denials will be based on inaccurate information.

As the proliferation of the SSN demonstrates, the creation of a national database to verify each American's eligibility to enter the work force will lead to increased sharing of information, increased demands for access for purposes other than the one the system was designed to support, and increased demands on individuals by third parties for access to this information -- a heavy price to ask all American's to pay and one that has not been justified by the problem of illegal immigrant workers.

The "worker verification" system proposals open the door to an Orwellian nightmare. Handing over the civil liberties of 98.5% of the American public is not the way to deal with the estimated 1.5% of the population that are illegal immigrants. In the final analysis, the establishment of a "worker verification registry," is a solution that threatens to create more serious problems than it solves. Given the tarnished history of national identification systems in America and other countries, the public distrust of data collection, and the extreme threat to civil liberties and civil rights posed by such systems, a

"worker verification" database should not be adopted as the "quick fix" to the problem of undocumented workers.

---

2) LETTER SENT FROM RIGHT-LEFT COALITION MEMBERS OPPOSING NATIONAL ID SYSTEMS.

May 23, 1995

Dear Member of Congress:
We are writing to express our concern that both Congress and the Administration are moving toward the implementation of a national worker registry. We believe such a plan put forward in the name of immigration control, is both misguided and dangerous for the following reasons:

It will not work. Those employers who rely on undocumented labor are already violating the law; they do so intentionally and are unlikely to use a verification system. Instead, they will continue to violate the law by hiring undocumented workers while employers who already comply with the law are subjected to new, costly requirements for the hiring process.

Faulty data. The data which a nationwide verification system would use would rely on two highly flawed data bases, one by the Social Security Administration (SSA) and the other the Immigration and Naturalization Service (INS~. Both are notorious for containing incorrect or outdated information, with error rates as high as 28 percent. Roughly 65 million Americans either enter the work force or change jobs every year. Even an error rate of no higher than one percent would mean that 650,000 Americans could be denied jobs every year.

An unfunded mandate on employers. The creation of a national verification system for every workplace in America would present a huge administrative burden to the nation's employers, especially small business. All employers would be required to ask the federal government's permission every time they want to hire somebody. Americans want fewer burdensome regulations, not new ones.

A threat to privacy and civil rights. Worker registry proposals ask Congress to create a database of personal information on all Americans and make it accessible to all employers. The openness of the proposed systems raises barriers to controlling and monitoring the use of information. Such systems are prone to abuse by persons who use it to selectively screen individuals whose appearance, surname or accent suggests they are foreign or to screen such persons outside of the context of employment. In addition, government often lacks the political will to limit access to information once collected. Indeed, other purposes for the data base are already being proposed, including verifying eli~ibility for public benefits, tracking childhood immunizations, and tracking child support payments. Once a system of information on all Arnericans is in place, it will inevitably become ubiquitous in American life, presenting an enormous threat to the privacy and liberty of Americans.

We believe it is unwarranted and unwise to create a data system involving 100 percent of Americans in an effort to identify the 1.5 percent who live illegally in the United States. We urge you to oppose the creation of a nationwide verification system.
Sincerely,

NATIONAL ORGANIZATIONS

American Civil Liberties Union (ACLU)
American Immigration Lawyers Association
Center for Democracy and Technology
Citizens for a Sound Economy
Immigration and Refugee Services of America
MALDEF, Los Angeles
National Asian Pacific American Legal Consortium
National Association of Korean Americans
National Council of La Raza
National Federation of Independent Business
Organization of Chinese Americans
Small Business Survival Committee
Southwest Voter Registration Education Project
U.S. Hispanic Chamber of Commerce

INDIVIDUALS

Martin Anderson, Hoover Institution
Stuart Anderson, Alexis de Tocqueville Institution
Ronald Bailey, Think Tank
Bernard Baltic, Reason Foundation
Douglas Bersharov, American Enterprise Institute
David Boaz, Cato Institute
Clint Bolick, Institute for Justice
Matthew Brooks, National Jewish Coalition
Phillip M. Burgess, Center for the New West
Merrick Carey, Alexis de Tocqueville Institute
Linda Chavez, Center for Equal Opportunity
Bryce Christensen, Editor, The Family in America
Jeff Eisenach, Progress & Freedom Foundation
Diana Furchtgett-Roth, American Enterprise Institute
Steve Gibson, Bionomics Institute
Stina Hans, Vista Hospital Systems
Robert B. Helms, American Enterprise Institute
Rick Henderson, Reason
John Hood, Bradley Fellow-Heritage Foundation
David Horowitz, Center for the Study of Popular Culture
Joseph J. Jacobs, Jacobs Engineering Group

Paul Jacobs, U.S. Term Limits
Kent Jeffreys, National Center for Policy Analysis
Thomas L. Jipping, Free Congress Foundation
Donna Kelsch, YMCA, NY
Jack Kemp, Empower America
Manuel S. Klausner, Kindel & Anderson
David Koch, Koch Industries
William Kristol, Project for the Republican Future
James P. Lucier, Jr., Citizens Against a National Sales Tax/VAT
John McClaughery, Ethan Allen Institute
Michael T. McMenaim, Walter & Haverfield
William H. Mellor III, Institute for Justice
Stephen Moore, Cato Institute
Reverend Craig B. Mousin, United Methodist Church of Christ
Richard S. Newcombe, Creators Syndicate
Grover Norquist, Americans for Tax Reform
Walter K. Olson, Manhattan Institute
Ellen Frankel Paul, Social Philosophy & Policy Center at Bowling Green State University
Jeffrey Paul, Social Philosophy & Policy Center, Bowling Green State University
Sally Pipes, Pacific Research Institute
Joyce Antilla Phipps, Clinical Professor at Seton Hall University Robert W. Poole, Jr., Reason Foundation
Steven R Postre, Graduate School of Management at the University of California at Irvine
Virginia Postrel, Reason Foundation
T.J. Rodgers, Cypress Semiconductor
Michael Rothschild, Bionomics Institute Rev. Don Smith
Dr. Christine Sierra, University of New Mexico
Julie Stewart, Families Against Mandatory Minimums Ron K. Unz, Wall Street Analytics
Richard J. Wilson, Professor, American University
Cathy Young, Women's Freedom Network
Benjamin Zycher, Department of Economics UCLA

LOCAL ORGANIZATIONS:

Albuquerque Border City Project
Asian Law Alliance
Asian Pacific American Legal Center of Southern California
Asylum and Refugee Rights Law Project
AYUDA
California Humane Development
Californians United for Equality
Center for Immigrant Rights
Chicago Coalition for Immigrant and Refugee Protection
Coalition for Humane Immigration Rights of Los Angeles (CHIRLA)
Coalition for Immigrant and Refugee Rights and

Services
Dominican Sisters of San Rafael, CA
El Centro Hispanoamerico, NJ
Immigrant Legal Resource Center, San Francisco
Immigrant's Rights Project
Immigration Law Project
Independent Women's Forum
International Assistance Program of Alabama, Inc.
International Institute of Los Angeles
Korean Youth and Community Center, Los Angeles
Lawyer's Committee for Civil Rights
Legal Assistance Foundation, Legal Services Center
Massachusetts Immigrant and Refugee Advocacy Coalition, Boston
New York Immigration Coalition, NY
North Texas Immigration Coalition of Dallas
Northwest Immigrant's Rights Project
Pacific Research Institute
Proyecto Adelante
Proyecto Libertad, Texas
Riverside Language Project, New York
Santa Clara County Network for Immigrant & Refugee Rights & Services
Sponsors to Assist Refugees, Portland, OR
Travelers and Immigrants Aid

---

3) CURRENT STATUS AND PATHS TO RELEVANT LEGISLATIVE DOCUMENTS

The sections of these bills pertaining to the Worker Verification Database
issue are available from CDT's ftp archive:

ftp://ftp.cdt.org/pub/cdt/policy/legislation/

s269 -- "The Immigrant Control and Financial Responsibility Act of 1995," introduced on January 24, 1995, by Senator Simpson (R-WY), Chairman of the Subcommittee, is scheduled for mark-up on June 6th;

s580 -- The "Illegal Immigration Control and Enforcement Act of 1995," introduced on March 21, 1995, by Senator Feinstein;

s754 -- The "Immigration Enforcement Improvements Act of 1995," introduced
on May 1, 1995, by Senators Kennedy, Simon and Boxer.

---

(4) ABOUT THE CENTER FOR DEMOCRACY AND TECHNOLOGY

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
###