

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF PENNSYLVANIA  
AMERICAN CIVIL LIBERTIES UNION, et al.,

v.

JANET RENO, Attorney General of  
the United States

CIVIL ACTION No. 96-963

---

AMERICAN LIBRARY ASSOCIATION,  
INC., et al.,

v.

UNITED STATES DEP'T OF JUSTICE,  
et al.

CIVIL ACTION No. 96-1458

Before: Sloviter, Chief Judge, United States Court of Appeals for the Third Circuit; Buckwalter and Dalzell,  
Judges, United States District Court for the Eastern District of Pennsylvania

June 11, 1996

ADJUDICATION ON MOTIONS FOR PRELIMINARY INJUNCTION

## **I. INTRODUCTION PROCEDURAL BACKGROUND**

Before us are motions for a preliminary injunction filed by plaintiffs who challenge on constitutional grounds provisions of the Communications Decency Act of 1996 (CDA or "the Act"), which constitutes Title V of the Telecommunications Act of 1996, signed into law by the President on February 8, 1996.(1) Telecommunications Act of 1996, Pub. L. No. 104-104, § 502, 110 Stat. 56, 133-35. Plaintiffs include various organizations and individuals who, inter alia, are associated with the computer and/or communications industries, or who publish or post materials on the Internet, or belong to various citizen groups. See ACLU Complaint (¶¶ 7-26), ALA First Amended Complaint (¶¶ 3, 12-33).

The defendants in these actions are Janet Reno, the Attorney General of the United States, and the United States Department of Justice. For convenience, we will refer to these defendants as the Government. Plaintiffs contend that the two challenged provisions of the CDA that are directed to communications over the Internet which might be deemed "indecent" or "patently offensive" for minors, defined as persons under the age of eighteen, infringe upon rights protected by the First Amendment and the Due Process Clause of the Fifth Amendment.

Plaintiffs in Civil Action Number 96-963, in which the lead plaintiff is the American Civil Liberties Union (the ACLU),(2) filed their action in the United States District Court for the Eastern District of Pennsylvania on the day the Act was signed, and moved for a temporary restraining order to enjoin enforcement of

these two provisions of the CDA. On February 15, 1996, following an evidentiary hearing, Judge Ronald L. Buckwalter, to whom the case had been assigned, granted a limited temporary restraining order, finding in a Memorandum that 47 U.S.C. § 223(a)(1)(B) ("the indecency provision" of the CDA) was unconstitutionally vague. On the same day, Chief Judge Dolores K. Sloviter, Chief Judge of the United States Court of Appeals for the Third Circuit, having been requested by the parties and the district court to convene a three-judge court, pursuant to § 561(a) of the CDA, appointed such a court consisting of, in addition to Judge Buckwalter, Judge Stewart Dalzell of the same district, and herself, as the circuit judge required by 28 U.S.C. § 2284.

After a conference with the court, the parties entered into a stipulation, which the court approved on February 26, 1996, wherein the Attorney General agreed that:

she will not initiate any investigations or prosecutions for violations of 47 U.S.C. § 223(d) for conduct occurring after enactment of this provision until the three-judge court hears Plaintiffs' Motion for Preliminary Injunction . . . and has decided the motion.

The Attorney General's commitment was qualified to the extent that:

her full authority to investigate or prosecute any violation of § 223(a)(1)(B), as amended, and § 223(d) as to conduct which occurs or occurred during any period of time after enactment of these provisions (including for the period of time to which this stipulation applies) should the Court deny plaintiffs' motion or, if the motion is granted, should these provisions ultimately be upheld.

Stipulation, ¶ 4, in C.A. No. 96-963.

Shortly thereafter, the American Library Association, Inc. (the ALA) and others<sup>(3)</sup> filed a similar action at C.A. No. 96-1458. On February 27, 1996, Chief Judge Sloviter, again pursuant to § 561(a) of the CDA and upon request, convened the same three-judge court pursuant to 28 U.S.C. § 2284. The actions were consolidated pursuant to Fed. R. Civ. P. 42(a), "for all matters relating to the disposition of motions for preliminary injunction in these cases, including the hearing on such motions."

The parties were afforded expedited discovery in connection with the motions for preliminary injunction, and they cooperated with Judge Dalzell, who had been assigned the case management aspects of the litigation. While the discovery was proceeding, and with the agreement of the parties, the court began receiving evidence at the consolidated hearings which were conducted on March 21 and 22, and April 1, 12 and 15, 1996. In order to expedite the proceedings, the parties worked closely with Judge Dalzell and arranged to stipulate to many of the underlying facts and to place much of their cases in chief before the court by sworn declarations, so that the hearings were largely devoted to cross-examination of certain of the witnesses whose declarations had been filed. The parties submitted proposed findings of fact and post-hearing memoranda on April 29, and the court heard extensive oral argument on May 10, 1996.<sup>(4)</sup>

## **STATUTORY PROVISIONS AT ISSUE**

Plaintiffs focus their challenge on two provisions of section 502 of the CDA which amend 47 U.S.C. §§ 223(a) and 223(d).

Section 223(a)(1)(B) provides in part that any person in interstate or foreign communications who, "by means of a telecommunications device,"<sup>(5)</sup> "knowingly . . . makes, creates, or solicits" and "initiates the transmission" of "any comment, request, suggestion, proposal, image or other communication which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age," "shall be criminally fined or imprisoned." (emphasis added).

Section 223(d)(1) ("the patently offensive provision"), makes it a crime to use an "interactive computer service"(6) to "send" or "display in a manner available" to a person under age 18, "any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such service placed the call or initiated the communication."

Plaintiffs also challenge on the same grounds the provisions in § 223(a)(2) and § 223(d)(2), which make it a crime for anyone to "knowingly permit[] any telecommunications facility under [his or her] control to be used for any activity prohibited" in §§ 223(a)(1)(B) and 223(d)(1). The challenged provisions impose a punishment of a fine, up to two years imprisonment, or both for each offense.

Plaintiffs make clear that they do not quarrel with the statute to the extent that it covers obscenity or child pornography, which were already proscribed before the CDA's adoption. See 18 U.S.C. §§ 1464-65 (criminalizing obscene material); id. §§ 2251-52 (criminalizing child pornography); see also *New York v. Ferber*, 458 U.S. 747 (1982); *Miller v. California*, 413 U.S. 15 (1973).

Plaintiffs in the ACLU action also challenge the provision of the CDA that criminalizes speech over the Internet that transmits information about abortions or abortifacient drugs and devices, through its amendment of 18 U.S.C. § 1462(c). That section now prohibits the sending and receiving of information over the Internet by any means regarding "where, how, or of whom, or by what means any [drug, medicine, article, or thing designed, adapted, or intended for producing abortion] may be obtained or made". The Government has stated that it does not contest plaintiffs' challenge to the enforceability of the provision of the CDA as it relates to 18 U.S.C. § 1462(c).(7)

As part of its argument that the CDA passes constitutional muster, the Government cites the CDA's "safe harbor" defenses in new § 223(e) of 47 U.S.C., which provides:

**(e) Defenses**

In addition to any other defenses available by law:

- (1) No person shall be held to have violated subsection (a) or (d) of this section solely for providing access or connection to or from a facility, system, or network not under that person's control, including transmission, downloading, intermediate storage, access software, or other related capabilities that are incidental to providing such access or connection that does not include the creation of the content of the communication.
- (2) The defenses provided by paragraph (1) of this subsection shall not be applicable to a person who is a conspirator with an entity actively involved in the creation or knowing distribution of communications that violate this section, or who knowingly advertises the availability of such communications.
- (3) The defenses provided in paragraph (1) of this subsection shall not be applicable to a person who provides access or connection to a facility, system, or network engaged in the violation of this section that is owned or controlled by such person.
- (4) No employer shall be held liable under this section for the actions of an employee or agent unless the employee's or agent's conduct is within the scope of his or her employment or agency and the employer (A) having knowledge of such conduct, authorizes or ratifies such conduct, or (B) recklessly disregards such conduct.

(5) It is a defense to a prosecution under subsection (a)(1)(B) or (d) of this section, or under subsection (a)(2) of this section with respect to the use of a facility for an activity under subsection (a)(1)(B) that a person --

(A) has taken, in good faith, reasonable, effective, and appropriate actions under the circumstances to restrict or prevent access by minors to a communication specified in such subsections, which may involve any appropriate measures to restrict minors from such communications, including any method which is feasible under available technology; or

(B) has restricted access to such communication by requiring use of a verified credit card, debit account, adult access code, or adult personal identification number.

(6) The [Federal Communications] Commission may describe measures which are reasonable, effective, and appropriate to restrict access to prohibited communications under subsection (d) of this section. Nothing in this section authorizes the Commission to enforce, or is intended to provide the Commission with the authority to approve, sanction, or permit, the use of such measures. The Commission shall have no enforcement authority over the failure to utilize such measures. . . .

## **II. FINDINGS OF FACT**

All parties agree that in order to apprehend the legal questions at issue in these cases, it is necessary to have a clear understanding of the exponentially growing, worldwide medium that is the Internet, which presents unique issues relating to the application of First Amendment jurisprudence and due process requirements to this new and evolving method of communication. For this reason all parties insisted on having extensive evidentiary hearings before the three-judge court. The court's Findings of fact are made pursuant to Fed. R. Civ. P. 52(a). The history and basic technology of this medium are not in dispute, and the first forty-eight paragraphs of the following Findings of fact are derived from the like-numbered paragraphs of a stipulation<sup>(8)</sup> the parties filed with the court.<sup>(9)</sup>

### **THE NATURE OF CYBERSPACE THE CREATION OF THE INTERNET AND THE DEVELOPMENT OF CYBERSPACE**

1. The Internet is not a physical or tangible entity, but rather a giant network which interconnects innumerable smaller groups of linked computer networks. It is thus a network of networks. This is best understood if one considers what a linked group of computers -- referred to here as a "network" -- is, and what it does. Small networks are now ubiquitous (and are often called "local area networks"). For example, in many United States Courthouses, computers are linked to each other for the purpose of exchanging files and messages (and to share equipment such as printers). These are networks.
2. Some networks are "closed" networks, not linked to other computers or networks. Many networks, however, are connected to other networks, which are in turn connected to other networks in a manner which permits each computer in any network to communicate with computers on any other network in the system. This global Web of linked networks and computers is referred to as the Internet.
3. The nature of the Internet is such that it is very difficult, if not impossible, to determine its size at a given moment. It is indisputable, however, that the Internet has experienced extraordinary growth in recent years. In 1981, fewer than 300 computers were linked to the Internet, and by 1989, the number stood at fewer than 90,000 computers. By 1993, over 1,000,000 computers were linked. Today, over 9,400,000 host computers worldwide, of which approximately 60 percent located within the United States, are estimated to be linked to the Internet. This count does not include the personal computers people use to access the Internet using modems. In all, reasonable estimates are that as many as 40 million people around the world can and do access the

enormously flexible communication Internet medium. That figure is expected to grow to 200 million Internet users by the year 1999.

4. Some of the computers and computer networks that make up the Internet are owned by governmental and public institutions, some are owned by non-profit organizations, and some are privately owned. The resulting whole is a decentralized, global medium of communications -- or "cyberspace" -- that links people, institutions, corporations, and governments around the world. The Internet is an international system. This communications medium allows any of the literally tens of millions of people with access to the Internet to exchange information. These communications can occur almost instantaneously, and can be directed either to specific individuals, to a broader group of people interested in a particular subject, or to the world as a whole.
5. The Internet had its origins in 1969 as an experimental project of the Advanced Research Project Agency ("ARPA"), and was called ARPANET. This network linked computers and computer networks owned by the military, defense contractors, and university laboratories conducting defense-related research. The network later allowed researchers across the country to access directly and to use extremely powerful supercomputers located at a few key universities and laboratories. As it evolved far beyond its research origins in the United States to encompass universities, corporations, and people around the world, the ARPANET came to be called the "DARPA Internet," and finally just the "Internet."
6. From its inception, the network was designed to be a decentralized, self-maintaining series of redundant links between computers and computer networks, capable of rapidly transmitting communications without direct human involvement or control, and with the automatic ability to re-route communications if one or more individual links were damaged or otherwise unavailable. Among other goals, this redundant system of linked computers was designed to allow vital research and communications to continue even if portions of the network were damaged, say, in a war.
7. To achieve this resilient nationwide (and ultimately global) communications medium, the ARPANET encouraged the creation of multiple links to and from each computer (or computer network) on the network. Thus, a computer located in Washington, D.C., might be linked (usually using dedicated telephone lines) to other computers in neighboring states or on the Eastern seaboard. Each of those computers could in turn be linked to other computers, which themselves would be linked to other computers.
8. A communication sent over this redundant series of linked computers could travel any of a number of routes to its destination. Thus, a message sent from a computer in Washington, D.C., to a computer in Palo Alto, California, might first be sent to a computer in Philadelphia, and then be forwarded to a computer in Pittsburgh, and then to Chicago, Denver, and Salt Lake City, before finally reaching Palo Alto. If the message could not travel along that path (because of military attack, simple technical malfunction, or other reason), the message would automatically (without human intervention or even knowledge) be re-routed, perhaps, from Washington, D.C. to Richmond, and then to Atlanta, New Orleans, Dallas, Albuquerque, Los Angeles, and finally to Palo Alto. This type of transmission, and re-routing, would likely occur in a matter of seconds.
9. Messages between computers on the Internet do not necessarily travel entirely along the same path. The Internet uses "packet switching" communication protocols that allow individual messages to be subdivided into smaller "packets" that are then sent independently to the destination, and are then automatically reassembled by the receiving computer. While all packets of a given message often travel along the same path to the destination, if computers along the route become overloaded, then packets can be re-routed to less loaded computers.
10. At the same time that ARPANET was maturing (it subsequently ceased to exist), similar networks developed to link universities, research facilities, businesses, and individuals around the world. These other formal or loose networks included BITNET, CSNET, FIDONET, and USENET. Eventually, each of these networks (many of which overlapped) were themselves linked together, allowing users of any computers linked to any one of the networks to transmit communications to users of computers on other networks. It is this series of linked networks (themselves linking computers and computer networks) that is today commonly known as the Internet.

11. No single entity -- academic, corporate, governmental, or non-profit -- administers the Internet. It exists and functions as a result of the fact that hundreds of thousands of separate operators of computers and computer networks independently decided to use common data transfer protocols to exchange communications and information with other computers (which in turn exchange communications and information with still other computers). There is no centralized storage location, control point, or communications channel for the Internet, and it would not be technically feasible for a single entity to control all of the information conveyed on the Internet.

## HOW INDIVIDUALS ACCESS THE INTERNET

12. Individuals have a wide variety of avenues to access cyberspace in general, and the Internet in particular. In terms of physical access, there are two common methods to establish an actual link to the Internet. First, one can use a computer or computer terminal that is directly (and usually permanently) connected to a computer network that is itself directly or indirectly connected to the Internet. Second, one can use a "personal computer" with a "modem" to connect over a telephone line to a larger computer or computer network that is itself directly or indirectly connected to the Internet. As detailed below, both direct and modem connections are made available to people by a wide variety of academic, governmental, or commercial entities.

13. Students, faculty, researchers, and others affiliated with the vast majority of colleges and universities in the United States can access the Internet through their educational institutions. Such access is often via direct connection using computers located in campus libraries, offices, or computer centers, or may be through telephone access using a modem from a student's or professor's campus or off-campus location. Some colleges and universities install "ports" or outlets for direct network connections in each dormitory room or provide access via computers located in common areas in dormitories. Such access enables students and professors to use information and content provided by the college or university itself, and to use the vast amount of research resources and other information available on the Internet worldwide.

14. Similarly, Internet resources and access are sufficiently important to many corporations and other employers that those employers link their office computer networks to the Internet and provide employees with direct or modem access to the office network (and thus to the Internet). Such access might be used by, for example, a corporation involved in scientific or medical research or manufacturing to enable corporate employees to exchange information and ideas with academic researchers in their fields.

15. Those who lack access to the Internet through their schools or employers still have a variety of ways they can access the Internet. Many communities across the country have established "free-nets" or community networks to provide their citizens with a local link to the Internet (and to provide local-oriented content and discussion groups). The first such community network, the Cleveland Free-Net Community Computer System, was established in 1986, and free-nets now exist in scores of communities as diverse as Richmond, Virginia, Tallahassee, Florida, Seattle, Washington, and San Diego, California. Individuals typically can access free-nets at little or no cost via modem connection or by using computers available in community buildings. Free-nets are often operated by a local library, educational institution, or non-profit community group.

16. Individuals can also access the Internet through many local libraries. Libraries often offer patrons use of computers that are linked to the Internet. In addition, some libraries offer telephone modem access to the libraries' computers, which are themselves connected to the Internet. Increasingly, patrons now use library services and resources without ever physically entering the library itself. Libraries typically provide such direct or modem access at no cost to the individual user.

17. Individuals can also access the Internet by patronizing an increasing number of storefront "computer coffee shops," where customers -- while they drink their coffee -- can use computers provided by the shop to access the Internet. Such Internet access is typically provided by the shop for a small hourly fee.

18. Individuals can also access the Internet through commercial and non-commercial "Internet service providers" that typically offer modem telephone access to a computer or computer network linked to the Internet. Many such providers -- including the members of plaintiff Commercial Internet Exchange Association -- are commercial entities offering Internet access for a monthly or hourly fee. Some Internet service providers, however, are non-profit organizations that offer free or very low cost access to the Internet. For example, the International Internet Association offers free modem access to the Internet upon request. Also, a number of trade or other non-profit associations offer Internet access as a service to members.

19. Another common way for individuals to access the Internet is through one of the major national commercial "online services" such as America Online, CompuServe, the Microsoft Network, or Prodigy. These online services offer nationwide computer networks (so that subscribers can dial-in to a local telephone number), and the services provide extensive and well organized content within their own proprietary computer networks. In addition to allowing access to the extensive content available within each online service, the services also allow subscribers to link to the much larger resources of the Internet. Full access to the online service (including access to the Internet) can be obtained for modest monthly or hourly fees. The major commercial online services have almost twelve million individual subscribers across the United States.

20. In addition to using the national commercial online services, individuals can also access the Internet using some (but not all) of the thousands of local dial-in computer services, often called "bulletin board systems" or "BBSs." With an investment of as little as \$2,000.00 and the cost of a telephone line, individuals, non-profit organizations, advocacy groups, and businesses can offer their own dial-in computer "bulletin board" service where friends, members, subscribers, or customers can exchange ideas and information. BBSs range from single computers with only one telephone line into the computer (allowing only one user at a time), to single computers with many telephone lines into the computer (allowing multiple simultaneous users), to multiple linked computers each servicing multiple dial-in telephone lines (allowing multiple simultaneous users). Some (but not all) of these BBS systems offer direct or indirect links to the Internet. Some BBS systems charge users a nominal fee for access, while many others are free to the individual users.

21. Although commercial access to the Internet is growing rapidly, many users of the Internet -- such as college students and staff -- do not individually pay for access (except to the extent, for example, that the cost of computer services is a component of college tuition). These and other Internet users can access the Internet without paying for such access with a credit card or other form of payment.

## **METHODS TO COMMUNICATE OVER THE INTERNET**

22. Once one has access to the Internet, there are a wide variety of different methods of communication and information exchange over the network. These many methods of communication and information retrieval are constantly evolving and are therefore difficult to categorize concisely. The most common methods of communications on the Internet (as well as within the major online services) can be roughly grouped into six categories:

- (1) one-to-one messaging (such as "e-mail"),
- (2) one-to-many messaging (such as "listserv"),
- (3) distributed message databases (such as "USENET newsgroups"),
- (4) real time communication (such as "Internet Relay Chat"),
- (5) real time remote computer utilization (such as "telnet"), and

(6) remote information retrieval (such as "ftp," "gopher," and the "World Wide Web").

Most of these methods of communication can be used to transmit text, data, computer programs, sound, visual images (i.e., pictures), and moving video images.

23. One-to-one messaging. One method of communication on the Internet is via electronic mail, or "e-mail," comparable in principle to sending a first class letter. One can address and transmit a message to one or more other people. E-mail on the Internet is not routed through a central control point, and can take many and varying paths to the recipients. Unlike postal mail, simple e-mail generally is not "sealed" or secure, and can be accessed or viewed on intermediate computers between the sender and recipient (unless the message is encrypted).

24. One-to-many messaging. The Internet also contains automatic mailing list services (such as "listservs"), [also referred to by witnesses as "mail exploders"] that allow communications about particular subjects of interest to a group of people. For example, people can subscribe to a "listserv" mailing list on a particular topic of interest to them. The subscriber can submit messages on the topic to the listserv that are forwarded (via e-mail), either automatically or through a human moderator overseeing the listserv, to anyone who has subscribed to the mailing list. A recipient of such a message can reply to the message and have the reply also distributed to everyone on the list.