A Post Mortem For The Communications Decency Act

Hal Berghel
University of Arkansas
hlb@acm.org

In a 7-2 decision last July, the U.S. Supreme Court struck down the CDA as too vague, too broad and in violation of the first amendment. It's hard to imagine how much more could be wrong with it. But it still has something of a life of its own - at least among the more socially conservative among us. In this article, we review some of the history behind the CDA, discuss some of the technologies commonly associated with it, and then try to derive some truths of enduring value from the experience.

Fears - Real And Imagined

We live in a complicated society. Those of us who are parents of young children are forever mindful of the real and present danger of child predators of all kinds. Little more than a year ago the U.S.' largest kiddie porn ring was prosecuted. Photographs of kidnaped children are prominently posted in our supermarkets and on our milk cartons. From a social point of view, these are not good signs. These are signs of a dysfunctional society.

In attempting to deal with these realities, the Clinton/Gore administration and Congress worked together to pass the so-called Exon Amendment to the 1996 Telecommunications Act - formally known as the 1996 Communications Decency Act. This aspect of the Telecommunications Act was the stuff of which the Supreme Court's negative judgment was made.

The Cda, The Whole Cda, And Nothing But The Cda

In their most basic form, the opposing views on the CDA seemed to be these:

(1) indecency in the Internet flourishes and puts our children at risk of being exposed to and harmed by pornography (among other things)

(2) indecency on the Internet is an anomaly. The Internet is no more dangerous than the Postal System in terms of the distribution of indecent material.

Motivated by position (1), Sen. James Exon of Nebraska put forth the CDA which:

- prohibited the use of "telecommunications devices" for 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..."
- "prohibited the display of information "in a manner available to persons under 18 years of age, ...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..."
- prohibited the transmission of information 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," via a modification of section 1462 of Title 18 of the U.S. Code. (note: This prohibition is difficult to ferret out because the CDA contains only a slight change of wording for section 1462, not the entire text of section 1462).

The CDA targeted content providers, and not service providers, for criminal prosecution. Violations of the CDA would have carried penalties of up to 2 years in prison and fines up to $100,000. The passage of the CDA galvanized many first amendment advocates, including, but not limited to, the ACLU, the National Writers Union, Human Rights Watch, the Electronic Frontier Foundation, the Electronic Privacy Information Center, Computer Professionals for Social Responsibility, the American Association of University Professors, the American Library Association, and Planned Parenthood, into petitioning a Federal court for a temporary restraining order and preliminary injunction against the Justice Department to prevent CDA's enforcement (A.C.L.U. v. Reno, 1996).

Enter The Supreme Court

In March of this year, the Communications Decency Act (CDA) was brought before the Supreme Court after the three-judge, U.S. District Court for Eastern Pennsylvania affirmed that:

(1) [the] Internet is "most participatory marketplace of mass speech that . . . the world has yet seen ... [and that] the empowering and non-invasive nature of the Internet make it a very different medium than radio or television,

(2) "...the use of the Internet is growing exponentially and, in part because of that increased use, the technology that governs the Internet is continuously and rapidly evolving,

(3) "...given the current state of technology, there is no way for the vast majority of Internet users to distinguish between adults and minors in their audience and, even in those parts of the Internet where it might be technologically possible, it is economically infeasible for many speakers, including the plaintiffs in this case. For these speakers, the

only way to ensure that minors do not have access to speech that might later be deemed "indecent" by a criminal jury is to eliminate such speech from the Internet entirely,

(4) "...less restrictive alternatives already exist that empower parents to make private decisions within the family about what materials their children should see.

The CDA, conversely, is uniquely ill-suited to shield children from sexually explicit material on the Internet precisely because it is a global communications medium. The record reveals that at least 40% of the speech now on the Internet originates overseas and the general consensus is that this percentage is growing. That speech can be accessed as easily as speech that originates domestically but, as the lower court found, and the government concedes, that speech is beyond the reach of our domestic criminal law."

This led the Federal three-judge panel to conclude that the CDA is unconstitutional and that enjoining a Federal statute in this case is warranted. This was the same view held by three other judges who had earlier passed on the CDA. Even members of the Justice Department felt that the Constitutionality of the CDA was in doubt.

Obscene Vs. Indecent

From a purely legal perspective, a great deal hinges on the label one attaches to the so-called "cybersmut." Since the Supreme Court's landmark decision, Miller v. California, in 1973, "obscene" material has been considered outside the realm of first amendment protections. On the other hand, "indecent" material has not been determined to be outside the purview of the first amendment. While I don't pretend to fully understand this distinction, it had serious legal consequences for the CDA.

In fact, the opposition to the CDA includes positions such as these:

- Indecency is a first amendment right. Indecent works may have socially redeeming characteristics, and may even pass the Miller v. California test,
- The vagueness of the terms of CDA - especially with regard to the term, indecent - are Constitutionally problematic, and enforcement may therefore violate the principle of due process, and
- some of the provisions of CDA, e.g. restricting access by credit card verification, etc., may not satisfy the "least restrictive means test" and thus be inconsistent with the first amendment.

Last July, the Supreme Court followed the lead of the lower Federal courts and struck down the entire CDA as unconstitutional. The court rejected the CDA's use of terms "indecent" and "offensive" as so broad as to be un-enforceable. It also found CDA's prohibitions to be in violation of first amendment rights. In addition, and what is likely to become more important in the long run, the Court found that the Internet should be regulated like publications and periodicals and not, as the Congress and Clinton Administration argued, like broadcast media. All courts found the digital network's potential to turn each end-user into a town crier so enticing, that they gave it the highest degree of first amendment protection - the same level afforded the news media.

Although the future of the CDA appears dim, it is not necessarily extinguished. However, further resurrections of CDA are likely to lack the support of the Clinton/Gore Administration, which appears to have lost interest in this losing cause. (As an aside, Germany currently has an Internet Law similar to the CDA.)

Technology To The Rescue?

One of the strongest arguments used by the detractors of the CDA was that modern technology can rescue us from the fear of cybersmut in the home and workplace, so the CDA is de facto unnecessary. The courts have even reasoned that filtering and blocking software may be effective in denying access to controversial sites to minors. For the past few years, technological tools for dealing with cybersmut have become fairly popular. We'll talk about two generic types of tools here: access controls and browser filters.

Perhaps the most important access control protocol for the Internet is the Platform for Internet Content Selection (PICS). PICS, a project supported by the World Wide Web Consortium in cooperation with major computer companies, has as its focal point the convergence of interests and objectives between supervisors (parents, employers, etc.) who wish to regulate information access and information-providers which want to "label" their products for maximal effect. Under PICS, supervisors would set the parameters of media filters in their "selection software" to block access to certain types of information. PICS is different from the existing selection software described above in that it defines a standard for labeling information, it is neutral with respect to specific filtering technologies.

The basic idea behind PICS is to define a standard for access-restriction and blocking that would spread industry-wide. If such a standard becomes reality, developers of filtering software would be able to rely on a single content description or labeling format.

PICS proposes the combined use of labeling schemes and various labeling services. The labels, or ratings, might be distributed in three ways:

(1) at the document level - by including a special "label" MIME-type in the headers of HTML documents which contains both label and the labeling service which distributes it,

(2) at the server level - by adding information on labeling services and document labels to the HTTP headers as they are sent by the server,

(3) by subscribing to third-party labeling services which would provide lists of URL's of "inappropriate" sites.

In each case, ancillary, meta-document information would be transmitted to the client which would report the rating(s) of the

information to be accessed. This information would then become the basis for blocking access to the information - in the Web browser, the TCP/IP protocol suite, or some form of intermediate proxy server or network firewall.

PICS - the leading candidate for the next generation of Web filtering protocols. http://www.w3.org/pub/WWW/PICS

PICS holds considerable promise as a "labeling infrastructure," because it presumes that actual ratings and ratings services will handled by third-party vendors. Over time, one might come to rely on certain ratings services and avoid others, giving the ratings game a dynamic character not unlike the Internet itself. This infrastructure could then complement collaborative filtering technology and recommender systems in separating users from inappropriate or unwanted information.

Browser tools are also becoming important information-filtering utilities. These tools monitor the user-client-server interaction for keywords, particular URLs, and keyboard activity. The server-to-client filtering can be done by reading the packet headers for listings of URLs which have been found offensive or unsuitable. The user-to-client filtering can be done by blocking the browser's navigation to selected sites by monitoring the typing taking place in the browser's "go to" text window. One of the products, Cyber Snoop, is depicted in Pearl Software's homepage.

One of the more robust Web filtering tools currently available. Incidentally, it also supports the PICS protocol. http://www.pearlsw.com

Such information filtering tools are touted as a great benefit in blocking unacceptable Web or Internet activities. Most are now designed to accommodate multiple users, import "censored" lists from third-party sources, can filter by keywords as well as URLs. With push technology near ubiquitous, automatic updates of such lists is trivial. Client-side tools also log Web navigation by user and protect sensitive files and lists with file locks.

What Has The Cda Taught Us?

What have we really learned of the CDA experience? I'm not sure that we've learned all that much.

For starters, it isn't clear to me that the Supreme Court really has much of a handle on the underlying technology issues. In the majority opinion the court claimed that they were very influenced by the use of the Web as a digital soapbox - "...each individual can become a pamphleteer..." Even if we admit that this is a social good, it is a very narrow perspective on the use of network technologies. The Internet also has multicast and broadcast components which are entirely different types of entities than distribution lists, news groups and political Web sites. These latter extensions could easily fall within first amendment protection under a reasonable interpretation where the former would not. To claim that Internet activities, as such and in general, should enjoy maximum first amendment privilege ignores some rather fundamental differences in the various uses of the technology. One person's first amendment privilege can become another's spam. Town crier's do not need un-solicited, push-phase multicasting.

Second, it is doubtful that conventional filtering and blocking software will ever achieve the goals that some detractors of the CDA claimed. At this writing, the meta-tag fields, titles and ratings schemes remain prescriptive in HTML documents. Produced by the information providers to advance their interests, it is naive to think that they would conform to standards and practices for Web indexing when there are legal and financial incentives not to do so. Think about it. Is it reasonable to expect that developers of a controversial sites to knowingly, and of their own accord, advertise the potentially illegal aspects of their sites in HTML document elements for which search engines (and hence, law enforcement) are sensitive. Filtering and blocking software may eventually do little more than draw attention to the boldest of pornographers, provocateurs, demagogues and perverts among us.

Third, site blocking by URL is also problematic. From a practical point of view, Web sites can re-locate with abandon over infinitely-dimensioned cyberspace. In addition, it isn't obvious that the preemptive blocking metaphor (ala PICS) offers a better alternative. Augmented with robust, client-side software, such standards could have a disquieting effect on all controversial communications. Society has a murky track record in the Motion Picture Association of America ratings, as motion pictures receive ratings based upon a small committee's tolerance of the gratuitous excesses in vogue. Depicted violence, un-imagined just

a generation ago, still find their way into films viewed by children. Why, we question, would this be different in home cable services or network information delivery systems. The filtering and blocking software now championed by the Clinton/Gore administration doesn't look like any silver bullet from this perspective.

Fourth, it remains unclear whether the CDA was ever about protecting children from cybersmut, for it made no provisions for parental responsibility and existing laws based on community standards. MSNBC columnist Brock Meeks suggests that "The CDA was never, ever about pornography or "smut" on the Internet, despite what 95% of all newspaper headlines inferred. Instead, the CDA was a cruel blunt instrument meant to further the political agenda of a self- absorbed "chosen few" that deemed themselves the guardians of our children and purveysors of All-American good tasted....The supporters of the CDA deemed themselves the guardians of my and your children." Like so many other social issues, the sensitive nature of the CDA debate made it vulnerable early on to emotionalism and politicization.

While one might be tempted to think that the current Supreme Court decision puts an end to the CDA matter, I think that this is unlikely. As the ancients felt moved to bring the licentious to art, modern cybernauts will continue to bring same to the Internet. This will, in turn, prompt others to seek legal or legislative remedy. In this scheme of things, the Internet is but another extending technology, rather than enabling one, which will be repeatedly subjected to the controversy. As its progenitor, the printing press, was drawn into the foray, so will the Internet. Meanwhile, each special-interest will include their own "index librorum prohibitorum" for like-minded cybernauts, and in so doing seek to advance the cause of censorship.

The CDA isn't dead yet. No doubt a "kindler and gentler" CDA will come forth someday which changes the legal playing field. As responsible computationalists we need to prepare for the inevitable by asking whether our experience with the CDA was enlightening and purposeful. I'm doubtful. ◆

For Further Reading

For an online version of the CDA see http://www.eff.org/pub/Censorship/Internet_censorship_bills/s652_hr1555_96_draft_bill.excerpt.

For information on CDA and the abortion issue, see http://www.eff.org/BlueRibbon/ab_debate.html and http://www.aclu.org/.

For information on the district court's verdict on the CDA, see http://www.epic.org/free_speech/CDA/lawsuit/affirm_motion_10_31.html). The Electronic Privacy Information Center (EPIC) at http://www.epic.org has extensive testimony on the CDA, press releases, alternative legislation, and copies of the court's decisions are available online at www.epic.org/free_speech/cda/lawsuit.

A summary of the decision by the Third Circuit Court of Appeals (Philadelphia) appears at www.access.digex.net/~epic/cda/highlights.html. Figures 1 and 2 depict the issues-oriented homepages of EPIC and the Electronic Frontier Foundation.

An *amici curiae* brief on behalf of many of the groups which oppose the CDA is at www.shsl.com/internet/supcourt/brief.html.

A highly-recommended overview of legal issues surrounding the Internet is to be found in Jonathan Rosenoer's *Cyberlaw: The Law of the Internet*, Springer_Verlag, 1997.

PICS is described at http://www.w3.org/pub/WWW/PICS/. A post-CDA debate between Neil Munro and Brock Meeks appeared in the September, 1997 issue of Communications of the ACM, pp. 25-28. Another article on this topic by the author may be found in the July, 1997 issue of the Communications of the ACM, pp. 11-15. A preprint of the latter is available online at http://www.acm.org/~hlb/col-edit/digital_village/jul-97/dv_7-97.html. Related materials and links may be found via the author's homepage at www.acm.org/~hlb/