Testimony before the Subcommittee on Telecommunications,
Trade, and Consumer Protection,
Committee on Commerce,
United States House of Representatives
September 11, 1998.

Lawrence Lessig
Jack N. and Lillian R. Berkman Professor for Entrepreneurial Legal Studies,
Harvard Law School.

I have reviewed the three legislative proposals presently before this Committee to address the concern about a minor's access to "harmful material" over the Internet. They each present different constitutional and policy questions, and I consider some of those questions in the few pages that follow. In my view, they all represent a careful attempt to deal with what many perceive to be a serious social problem. They each approach the issue in a slightly different way, and they are all more respectful of our free speech tradition than was the Communications Decency Act of 1996.[1]

In my view, however—and even for those who believe most strongly that Congress should act to protect children in this context—it would be a mistake to enact this legislation just now. The architectures of the Internet are changing at a dramatic pace, and, as I explain more carefully below, if Congress were to act now, it would risk entrenching a less efficient or effective technology for dealing with the problem that it seeks to address. Acting now, in other words, risks defeating the very objective that these proposals seek to achieve—namely effective parental control over the material to which their children are exposed.

My argument is not that Congress should do nothing. There are serious questions about the nature of this problem that Congress should, through hearings, seek to resolve. This is an appropriate role for Congress in the midst of the present revolution. But until we know more about how the Internet will develop, we should not pass laws that entrench technologies that may, in a very short time, no longer be necessary or effective.

H.R. 3783—Child Online Protection Act

This proposal is a careful response to the Supreme Court's decision in *Reno* v. *ACLU*.[2] Unlike the Communications Decency Act of 1996, the bill is targeted at commercial speech that is "harmful to minors." The pedigree for state regulation of such speech is well established.[3] As Justice O'Connor indicated in her concurring opinion in *Reno*, many states rely upon very similar

---

[1] 110 Stat. 56.

[2] 117 S.Ct. 2329 (1997).

[3] Its source is *Ginsberg* v. *New York*, 390 U.S. 629 (1968).

language to regulate the display and distribution of adult material.[4] In light of this authority, my view is that this bill could well be judged constitutional.

There are, however, a number of technical problems with the bill that do raise significant constitutional questions. There is as well a more fundamental problem that in my view makes this legislation unadvisable at the present time. I consider the second point first.

The essence of the bill is a proscription against the distribution to minors of matter that is "harmful to minors," tied to a defense for sites that screen access using a number of adult identification systems, or proxies for adult identification systems (such as credit cards.) The basic structure is zoning, and the constitutionality of such zoning depends upon minimizing the burden that the regulation imposes upon those who have a constitutional right to the speech at issue.[5]

In their present form, however, adult identification systems are significantly burdensome. This burden has three dimensions. First, they all are essentially password systems that are cumbersome to use and relatively expensive to maintain. This feature was most important to the Court in *Reno*. As an adult "surfs" through adult sites, he or she is potentially forced to present a series of different "IDs" to gain access to constitutionally protected speech.

Second, these systems interfere with an individual's ability to access adult material anonymously. All the systems identified in the proposal tie age verification to the identity of an individual, meaning that they all, to some degree, require that individuals give their name as a condition to getting access to constitutionally protected speech. But there is no way that an individual can know how that information will be used by the site, or by an ID company. And the temptation for such organizations subsequently to sell the names of individuals to email spam organizations, or others, is great.

Third, the most common form of identification—the credit card—creates a related and significant risk of abuse itself. Often a

---

[4] 117 S.Ct., at 2352 (O'Connor, concurring).

[5] *Id.*, at 2353.

site will promise that credit card information will be used only for identification purposes. But because it is so easy for the consumer to lose control over credit card information in cyberspace, the consumer faces a risk that the data he or she provides so as to get access to a site will be used improperly later on. (I have heard of one site, for example, that promises to charge a credit card just $1 to access an adult material, but in the fine print of the agreement, the site claims the right to charge the user $20 a month if the user does not cancel the subscription after 72 hours, and further threatens that canceling at the appointed time is the only way to cancel a subscription.)

If these architectures of identification were the only possible way in which the government's interest in zoning "harmful material" from kids could be accomplished, then these burdens might be permissible under the Court's test in *Reno*.[6] But they are not the only feasible technologies. One alternative—which would be less burdensome to the user, and which could assure anonymity and avoid the risks that credit cards present—would be digital certificate technologies.[7] With such certificates, one in principle could certify one's age without revealing other facts—such as one's name, or credit information—and this certification could be done invisibly, or automatically, when a browser connected with a given site.

The digital certificate industry, however, is just in its infancy. The market is still groping for a model for certificates, and it is unclear now which form makes most sense. At this stage, for Congress to push an outdated identification technology could significantly interfere with the development of these preferable and more protective alternatives. Only when these technologies have matured can Congress make a sensible judgment about the kinds of identification it can, and should, require.

In addition to this general problem with the proposal, there are a number of more specific concerns as well.

---

[6] See Eugene Volokh, *Freedom of Speech, Shielding Children, and Transcending Balancing*, 1998 Sup. Ct. Rev. 31, 38-39 (1998).

[7] See the description in A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 Or. L. Rev. 49 (1996).

- §(e)(1), in §3(a) of the proposal, extends the proscription to those "in the business of selling *or transferring* … material that is harmful to minors." It is unclear who is included by the term "transferring." One could well read the proposal to reach any Internet Service Provider that helped facilitate the transfer of such material, whether or not that ISP made such business its primary concern.

- §(e)(2),(3) are both criminal provisions, one directed against those who intentionally violate the proscription paragraph, and the other against those who simply "violate[]" the proscription paragraph. In my view, a criminal penalty in this context creates too great a chill on legitimate speakers. At most the statute should provide a civil remedy.

- §(e)(7)(A) defines the "World Wide Web" to include "hypertext transfer protocol, file transfer protocol, or other similar protocols." It is unclear how far the clause "other similar protocols" is intended to reach. USENET, for example, is a set of protocols for exchanging messages in a public fashion. Its protocols don't now include a way to authenticate on the basis of age.[8] The bill should be clarified to specify how far it is intended to reach.

- §(e)(7)(D) defines "harmful to minors" by a modified statement of the *Ginsberg* test—modified in light of *Miller* v. *California*.[9] But the test as modified does not take account of community standards in setting the test of "harmful," as the standard for obscenity does.[10]

- §3(b) requires that the FCC post "information as is necessary to inform the public of the meaning of the term …harmful to minors." But in light of the Supreme Court's

---

[8] Though there are proposals that the protocol be changed to enable such authentication. See Stan Barber, *Internet Draft, Network News Transfer Protocol* (March 1998), available at ftp://ftp.ietf.org/internet-drafts/draft-ietf-nntpext-base-04.txt.

[9] 413 U.S. 15 (1973).

[10] *Id.*

> decision in *Bantam Books* v. *Sullivan*,[11] it is clear that the FCC's power here is quite limited. The statute should specify more clearly just what kind of information it intends the FCC to post, and indicate clearly that these postings are not to become the equivalent of a "blacklist" of material.

H.R. 3177—Safe Schools Internet Act of 1998

This proposal requires, as a condition of receiving federal funding, that "elementary or secondary school[s and] librar[ies]" certify that they have a "system" to "filter or block matter deemed to be inappropriate for minors." "Inappropriate" is to be determined, under the bill, by local school or library officials, and the bill would not allow the judgment of these local officials to be second-guessed by any agency of the federal government. Presumably, so long as the local officials have made a selection, certification would be assured.

The problem with this proposal, however, is similar to the problem with H.R. 3783. For the bill seems to presume that technology exists that would allow local officials to make subtle choices about the kinds of material the software will filter. But in fact, the technology of filtering is not now so well developed. Given the present array of blocking and filtering software, the local official in effect would be forced to delegate this decision about the kinds of material to be blocked to software companies that are now independently marketing the material to parents.

This technologically forced delegation raises significant constitutional concerns. For the scope of material that is presently blocked by blocking software typically extends far beyond the speech that governments can constitutionally restrict. The speech blocked by such programs reaches far beyond the narrow scope of "harmful to minors," and, in some cases, well beyond the reach of the Communications Decency Act of 1996. Congress would then be indirectly forcing (through the spending power) local governments to impose conditions on speech access inconsistent with First Amendment principles.[12]

---

[11] 372 U.S. 58 (1963).

[12] Given the Supreme Court's standard of review in spending clause cases, see, e.g., *South Dakota v. Dole*, 483 U.S. 203 (1987), my claim is not that this provision would necessarily be struck by the Court. But Congress has an

Once again, the better solution would be to allow the technologies of filtering to develop, before Congress in effect mandates their use. There is a wide range of new technologies for rating and filtering speech now being developed in the market. Congress again would be better advised to let those technologies mature before pushing localities to use them.

H.R. 774—Internet Freedom and Child Protection Act of 1997

This proposal would require "access providers" to offer—either for a fee or at no charge—"screening software that is designed to permit the customer to limit access to material that is unsuitable for children." In my view, there is nothing constitutionally troubling about this provision, though I can't see what problem it is meant to solve.

There are many kinds of access providers—some focused on families, others on business. Presumably, these providers have a sufficient incentive to provide services that their customers demand. To satisfy the requirements of this bill, all providers would have to provide child protection software—whether the customer was Citibank or the family next door. But it not clear what advantage is gained by giving Citibank the option to buy child protection software, and it is unclear why a family access provider won't do so on its own.

Indeed, the major access providers already comply with the requirements of this bill. America Online has an extensive system of protection that it offers its customers; presumably, any other access provider could comply by simply providing a link on its web page to vendors that sold child protection software. Given the ease with which suppliers now meet market demand, it is uncertain what positive function the regulation would have.

---

independent duty to consider constitutional norms in the spending clause context, and these norms of federalism should be more robust than those considered by the Supreme Court.