THE NEW ATLANTIS
A Journal of Technology & Society

Porn, Privacy, and Kids

Congressional Attempts to Make the Internet Child-Friendly

Crafting legislation to protect children from the potential evils of the Internet has largely been a process of trial and error. Thus far, Congress has drafted no fewer than eleven different statutes—but only a few have survived judicial scrutiny. Lawmakers are giving it another try this year.

The first law to address children and the Internet, the Communications Decency Act (CDA) of 1996, made it a crime to use a telecommunications device to transmit "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"—with penalties of up to two years in jail and fines of $250,000. Soon after it was signed into law, the American Civil Liberties Union and 18 other watchdog groups filed suit, claiming that the law violated the First and Fifth Amendments. When the case reached the Supreme Court, the ACLU won with a 7-2 ruling that the law "place[d] an unacceptably heavy burden on protected speech." Writing for the majority, Justice John Paul Stevens argued that the CDA failed to distinguish between sexually explicit speech that has social or artistic value and pornographic speech. The law, Stevens wrote, was not the "least

restrictive" means by which Congress could prevent transmission of indecent materials to a minor.

In response, lawmakers drafted the 1998 Child Online Protection Act (variously known as COPA or "CDA II"). Tailored more narrowly than the original CDA, the new law targeted only commercial entities on the Internet. It required that they use identification systems—like a credit card number—to keep minors from accessing obscene materials online.

The new law, however, failed to allay the concerns of the Supreme Court. The ACLU and several other organizations challenged COPA the day after President Clinton signed the bill. The Court ruled in an 8-1 decision last year that the law was too broad in scope and could not be practically enforced. The law was sent back to a lower court for review, and it was again struck down as unconstitutional in March of 2003.

In the meantime, members of Congress drafted at least three additional pieces of legislation, all characterized as "Sons of CDA," none of which were enacted into law. In 2000, Congress settled on the Children's Internet Protection Act (CIPA), which blocked federal funds for schools and public libraries unless they employed software to filter out material deemed harmful to minors. The law instantly raised the ire of free speech advocates, who argued, with some justification, that the filters would block harmless sites and would force adults to ask permission to gain access to blocked sites. The ACLU and American Library Association soon challenged the law. This time the Supreme Court's decision, announced in June 2003, came down in favor of the statute; in a 6-3 vote, the Court held that if the government provides funds for a program, it is entitled to set parameters for the operation of that program.

Laws prohibiting the spread of online child pornography have had almost as complicated a legal history as the "Sons of CDA." The Child Pornography Prevention Act (CPPA) was enacted in 1996 to combat virtual child pornography. CPPA banned the possession of any computer-generated image which "is, or appears to be, of a minor engaging in sexually explicit conduct." A free speech advocacy group filed suit on the grounds that the law was overbroad—that is, that CPPA would endanger constitutionally protected speech.

In the Supreme Court's April 2002 decision, Justice Anthony Kennedy wrote that restrictions on sexually explicit materials would endanger the performance of literary works depicting teen sexuality, such as *Romeo and Juliet*. "Shakespeare may not have written sexually explicit scenes for the Elizabethan audience," Kennedy argued, "but were modern directors to adopt a less conventional approach, that fact alone would not compel the conclusion that the work was obscene." The Court thus decided that only pornography with actual children—as opposed to fake or computer-generated child porn—could be outlawed under the First Amendment.

In the wake of the Court's decision, the number of defendants claiming that the child pornography found on their computers is fake has increased, according to the Justice Department. This "virtual porn defense" has made prosecutors' work much more difficult, as they must now show that defendants' pornographic images depict actual children. In one case, a judge even held that the government must prove that the defendant actually *knew* that pornographic images depict real children—a nearly impossible task.

In response, Congress this year—in a show of truly staggering acronymic acu-

men—passed the Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today (PROTECT) Act. The PROTECT Act makes it more difficult for defendants to use the virtual porn defense in court. The act also makes it a crime to use a misleading Internet domain name with the intent to trick a minor into viewing obscene materials. Even though the PROTECT Act was written to survive judicial review, several legal commentators have suggested it will meet the same fate as its predecessor.

Congress has had slightly more success protecting the privacy of children on the Internet. After a number of high-profile cases in which investigators demonstrated the vulnerability of children's privacy online (in one case, a CBS reporter purchased a list of children's names and addresses while pretending to be an infamous child killer), Congress in 2000 passed the Children's Online Privacy Protection Act (COPPA), which requires that website operators obtain proof of parental consent before collecting personal information from children younger than 13.

Since verifying parental permission is an onerous undertaking in a medium known for anonymity and fraud, several legitimate websites that once catered to kids disappeared after COPPA was enacted. Even today, several major businesses are still having trouble getting the hang of the privacy law. Two companies that operate websites directed to children—Mrs. Fields Cookies and Hershey Foods Corporation—had to pay tens of thousands of dollars this year after the Federal Trade Commission charged that they collected personal information from thousands of children without first getting parental permission. And just a few months ago, the FTC received complaints that Amazon.com was using a disclaimer to the effect that its site is intended only for adults, even though it allows minors to post reviews containing personal information.

Yet another congressional experiment relating to children and the Internet is just now getting underway. Starting this summer, web addresses ending with ".kids.us" will be available to anyone willing to scrub from their site all mature content, pornography, inappropriate language, and hate speech, as well as anything involving violence, drugs, alcohol, tobacco, gambling, weapons, or criminal activity.

While these restrictions might raise some First Amendment concerns, a more immediate and practical question is whether the decency guidelines for the kids.us domain can be monitored and enforced effectively and fairly. It remains to be seen whether NeuStar, the Virginia-based company in charge of the kids.us domain, will be capable of providing "access only to material that is suitable for minors and not harmful to minors," as Congress has required.