

5 Freedom of Speech in Cyberspace

5.1 Changing Communications Paradigms

The global nature of the Web interacts with different laws and levels of freedom of speech in different countries.

REGULATORY PARADIGMS

Mike Godwin with the Electronic Frontier Foundation:

It is a medium far different from the telephone, which is only a one-to-one medium, ill-suited for reaching large numbers of people. It is a medium far different from the newspaper or TV station, which are one-to-many media, ill-suited for feedback from the audience. For the first time in history, we have a many-to-many medium, in which you don't have to be rich to have access, and in which you don't have to win the approval of an editor or publisher to speak your mind. Usenet and the Internet, as part of this new medium, hold the promise of guaranteeing, for the first time in history, that the First Amendment's protection of freedom of the press means as much to each individual as it does to Time Warner, or to the Gannett, or to the *New York Times*.

Historically in the U.S., communications technologies were divided into three categories with respect to the degree of First Amendment protection and government regulation:

- Print media (newspapers, books, magazines, pamphlets).
- Broadcast (television, radio).
- Common carriers (telephone, telegraph, and the postal system).

Broadcasting licenses are selected by the government and must meet government standards of merit, a requirement that would not be tolerated for publishers because of the obvious threat to freedom of expression.

The argument now used to justify government-imposed restrictions on content is that broadcast material comes into the home and is difficult to keep from children.

The Internet and ultimately the World Wide Web became major arenas for distribution of news, information, and opinion. Various political forces are fighting over the issue of control versus freedom. Because of the immense flexibility of computer communications systems, they do not fit neatly into the publishing, broadcasting, and common carriage paradigms.

It remains uncertain what degree of censorship and regulation of speech will apply to the Internet and the Web. In 1996, the main parts of the first major Internet censorship law, the Communications Decency Act (CDA), were ruled unconstitutional.

Censorship decisions in other countries will have an impact on Internet content.

The First Amendment was written precisely for offensive and/or controversial speech and ideas; it would not be needed to protect speech and publication that no one objected to. The First Amendment covers spoken and written words, pictures, art, and other forms of expression of ideas and opinions (including, for example, wearing armbands to express support of a political cause). The First Amendment is a restriction on the power of government, not individuals or private business. Rejection or editing by a publisher is not a violation of a writer's First Amendment rights.

Anonymous speech has been protected in many court decisions, but there are serious attempts to limit or prohibit anonymity on the Internet.

When the government pays, it can choose to restrict speech that would otherwise be constitutionally protected.

5.2 Offensive Speech and Censorship in Cyberspace

5.2.1 What Is There? What Is Illegal?

What is offensive speech? What should be prohibited or restricted by law in cyberspace? The answer depends on who you are. It could be political or religious speech, pornography, sexual or racial slurs, Nazi materials, libelous statements, abortion information, anti abortion information, advertising of alcoholic beverages, advertising in general, depictions of violence, or violence, or information about how to build bombs.

Pornography online is a multibillion-dollar business with sites worldwide.

Sexual material quickly invades all new technologies and art forms.

From cave paintings to frescos in Pompeii to stone carvings at Angkor Wat, erotica have flourished.

Pornography is debated endlessly.

We try to focus specifically on new problems and issues related to computer systems and cyberspace.

Inappropriate material can be easier for children to get on the Web, and problematic material spreads more easily and anonymously.

WHAT WAS ALREADY ILLEGAL?

Child pornography includes pictures or movies of actual minors (children under 18) in sexual positions or engaged in sexual acts. It has long been illegal to create, possess, or distribute child pornography, primarily because its production is considered abuse of the actual children.

In 1996, Congress passed the Child Pornography Prevention Act to extend the law against child pornography to include “virtual” children, that is computer-generated images that appear to be minors as well as other images where real adults appear to be minors. After conflicting federal appeals court decisions about whether the law violated the First Amendment, the Supreme Court ruled, in 2002, that it did.

5.2.2 Material Inappropriate for Children

There is no doubt that there is material on the Web that most people would consider inappropriate for children.

There is much on the Web that is extremely offensive to adults. It is not surprising that some people see the Internet as a scary place for children.

HOW THE TECHNOLOGY CHANGES THE CONTEXT

If a young child tried to buy a ticket for an X-rated movie or to buy an adult magazine, a cashier would see the child and refuse. On the Web, a child can access pornography without an adult observer.

The anonymity of the Net makes it easier for people to prey on children.

Schools and libraries used to be relatively safe havens from pornography and violent or hateful materials. The introduction of Internet terminals allows entrance of the undesirable material.

PROTECTING CHILDREN

Child pornography is illegal, and it is illegal to lure children into sexual acts.

Are new restrictions on freedom of speech needed to protect children on the Internet?

America Online, warns that, when subscribers notify the company of illegal activity, AOL reports it to the FBI and complies with subpoenas.

AOL lets parents set up accounts for their children without e-mail, or with a specified list of addresses from which e-mail will be accepted.

Software filtering products with names such as Cyber Patrol, X-Stop, SurfWatch, and Net Nanny block access to sites that contain material that might be inappropriate for a child.

When mandated for schools and libraries, filters are much more controversial.

One of the best ways to protect children is good parenting.

5.2.3 Censorship Laws

THE COMMUNICATIONS DECENCY ACT

In 1995, the FBI reported that “utilization of online services or bulletin-board systems is rapidly becoming one of the most prevalent techniques for individuals to share pornographic pictures of minors, as well as to identify and recruit children into sexually illicit relationships.”

Increasing publicity and political pressure led Congress to pass the Communications Decency Act of 1996 (CDA).

A broad collection of organizations, businesses, and individuals sued to block it. Two federal courts and the Supreme Court (in 1997) ruled unanimously, in *American Civil Liberties Union et al. V. Janet Reno*, that the censorship provisions of the CDA were unconstitutional.

The decisions against the CDA established that “the Internet deserves the highest protection from government intrusion.”

The difficulty in determining what to censor is illustrated by America Online’s action in response to government pressure to prohibit obscene or vulgar language. AOL included the word “breast” in its list of words banned from subscriber profiles. A week later the ban was reversed after protest, ridicule, and outrage from breast-cancer patients.

It is sometimes difficult to design a law that keeps inappropriate material from children while allowing access for adults.

When the government is pursuing a legitimate goal that might infringe on free speech (in this case, the protection of children), it must use the least restrictive means of accomplishing the goal.

THE CHILD ONLINE PROTECTION ACT

Congress tried again, with the Child Online Protection Act (COPA), passed in 1998. Sites with potentially “harmfully” material would have to get proof of age from site visitors. First Amendment supporters argued that the law was too broad and would threaten art, news, and health sites. A federal appeals court agreed, in 2000, that the censorship provisions of the law were unconstitutional.

THE CHILDREN’S INTERNET PROTECTION ACT

In 2000, Congress passed the Children’s Internet Protection Act (CIPA). It applies only to schools and libraries that participate in certain federal programs. It requires that such schools and libraries install filtering software on all Internet terminals to block access to sites with child pornography, obscene material, and material “harmful to minors.”

5.2.4 Internet Access in Libraries and Schools

PROBLEMS WITH FILTERS

Software filters work in a variety of ways. They can block sites with specific words or phrases. They can block sites according to various rating systems. They can contain long lists of specific sites to block.

It should be obvious that filters cannot do a perfect job. In fact, many do a very poor job.

Various studies have shown that filters block numerous innocent, legal sites for no apparent reason.

None of the solutions we describe in this book for problems generated by new technologies are perfect. They have strengths and weaknesses and are useful in some circumstances and not others.

PROBLEMS IN LIBRARIES

The authors of CIPA attempted to avoid the courts’ rejection of the CDA and COPA. The Supreme Court had not yet ruled when this book was being written.

5.2.5 Talking About Bombs—or Farming

There are many similarities between the controversy about bomb-making information on the Net and the controversy about pornography. As with pornography, bomb-making information is already widely available in traditional media, protected by the First Amendment.

Because of the conflict with the First Amendment, there was no federal law against bomb information on the Internet until 1999—after the shootings at Columbine High School in Littleton, Colorado. Congress passed a law mandating 20 years in prison for anyone who distributes bomb-making information knowing or intending that it will be used to commit a crime.

5.2.6 Challenging Old Regulatory Paradigms and Special Interests

Quicken and Nolo Press sell self-help legal software to assist people in writing wills, premarital agreements, and many other documents.

A Texas judge banned Quicken legal software from Texas in 1999.

The judge decided the software amounted to the practicing of law without a Texas license. (The Texas legislature later changed its law to exempt software publishers.)

The Web provides the potential for reducing prices of many products by eliminating the “middleman.” Small producers who cannot afford expensive distributors or wholesalers can set up a Web site and sell directly to consumers nationwide—but not if they operate a small winery. Twenty-nine states in the U.S. have laws restricting the shipping of out-of-state wines directly to consumers.

State governments argue that the laws are needed to prevent sales to minors.

Lawsuits in several states are challenging the laws against out-of-state wine shipments.

If these suits are successful, this will be another instance where the Web leads to removal of longstanding restrictions on freedom of speech and commerce.

5.2.7 Censorship on the Global Net

THE GLOBAL IMPACT OF CENSORSHIP

For a long time, the “conventional wisdom” among most users and observers of the Net was that the global nature of the Net is a protection against censorship. Web sites with content that is illegal in one country can be set up in some other country.

E-mail and fax machines played a significant role during the collapse of the Soviet Union and the democracy demonstrations in China’s Tiananmen Square.

In general, access to information and communications decreases a government’s ability to abuse its people.

In some ways however, the globalness of the Net makes it easier for one nation to impose restrictive standards on others.

Governments are finding ways to use new technology to prevent their citizens from accessing prohibited material.

In 1955, German prosecutors told CompuServe to block access by German subscribers to newsgroups with indecent and offensive material.

In 2000, a French court ordered Yahoo! To block access by French people to Yahoo!’s U.S.-based auction sites where Nazi memorabilia was sold.

It was widely viewed as a threat to freedom of speech.

Shortly after the French court issued their order, Yahoo! Announced that it would ban “hate material,” including Nazi and Ku Klux Klan memorabilia, from its auction sites.

Ebay also announced a ban on memorabilia about Nazis, the Ku Klux Klan, and other hate groups.

Free-speech advocates worried that the policy changes demonstrate the power of one government to impose its censorship standards on other countries.

If Web sites must comply with the laws of 180 countries, what would happen to the openness and global information flow of the Web?

CENSORSHIP IN OTHER NATIONS

The vibrant communication made possible by the Internet threatens governments in countries that lack political and cultural freedom.

In countries where criticism of the government is illegal or not tolerated, searches for “countersocial activity” have ominous implications.

In 1996, Pakistan banned Internet telephony. In 2000, Burma (Myanmar) banned use of the Internet or creation of Web pages without official permission, posting of material about politics, and posting of any material deemed by the government to be harmful to its policies.

Internet access was prohibited in Eritrea.

The government of Iran made people dismantle satellite dishes to avoid “cultural contamination” from U.S. television.

China channeled all foreign Internet traffic through a small number of gateways under its control.

A Chinese Internet entrepreneur was sentenced to two years in jail for sharing e-mail addresses with a pro-democracy Internet journal based in the United States.

5.3 Anonymity

5.3.1 *Common Sense and the Internet*

Jonathon Swift published his humorous and biting political satire *Gulliver’s Travels* anonymously.

In the nineteenth century, when it was not considered proper for women to write books, women writers such as Mary Ann Evans and Amantine Lucile Aurore Dupin published under male pseudonym.

On the Internet, people use pseudonyms (“handles,” aliases, or screen names) to keep their real identity private. Victims of rape and of other kinds of violence and abuse and users of illegal drugs who are trying to quit are among those who benefit from a forum where they can talk candidly without giving away their identity.

Whistleblowers may choose to release information via anonymous postings.

To send anonymous e-mail, one sends the message to a remailer service, where the return address is stripped off and the message is resent to the intended recipient.

Several businesses, like Anonymizer.com and Zero-Knowledge Systems, provide a variety of sophisticated tools and services that enable us to send e-mail and surf the Web anonymously.

5.3.2 Is Anonymity Protected?

What happens when someone wants to know the real identity of a person who posted something? How well protected are our real identities?

POLITICAL SPEECH

The Web enables anyone to express political opinions to a wide audience inexpensively. The Supreme Court has repeatedly ruled that the right to speak anonymously.

Regulations of the Federal Election Commission (FEC) restrict anonymity.

A man set up a Web page satirizing the governor of his state.

The FEC told the first man that he might have to comply with federal campaign laws requiring that he identify himself on the Web site and file financial statements.

The Web reopens the issue of conflicts between campaign regulations and freedom of speech.

CRITICIZING CORPORATIONS

Businesses have two areas of legitimate complaints: postings that spread false and damaging rumors, and postings that include confidential business documents or other proprietary information.

A former employee posted particularly nasty comments about a company and its executives, including charges of adultery. When sued, he apologized and said he made it all up. We are not exempt from ordinary ethics and defamation laws merely because we are using the Internet or signing comments with an alias rather than a real name.

Should businesses be able to get real names of people posting messages they object to? If a service gives out someone's real name, should the person be informed?

Gradually, as more attention is focused on the threats to free speech, some courts rejected some subpoenas for real names.

5.3.3 Against Anonymity

Esther Dyson, "anonymity is the opposite of community."

Commenting on a lawsuit challenging Georgia's anti-anonymity law, Dyson said, "Anonymity shouldn't be a crime. Committing crimes should be a crime."

Because of its potential to shield criminal activity or because they consider it incompatible with politeness and netiquette (online etiquette), some services choose to discourage or prohibit anonymity.

LAWS AGAINST ANONYMITY

Anonymity on the Internet is used for criminal and antisocial purposes. It is used for fraud, harassment, and extortion. It is used to distribute child pornography, to libel or threaten others with impunity, and to infringe copyrights by posting and downloading copyrighted material without authorization. It can be used to plan terrorist attacks. Like encryption, anonymity technology poses strong challenges to law enforcement. Anonymity makes it difficult to track criminals and terrorists.

Does the potential for harm by criminals who use anonymity to hide from law enforcement outweigh the loss of privacy and restraint on freedom of speech for honest people who use anonymity responsibly? Is anonymity an important protection against possible abuse of power by government? Should people have the right to use available tools, including strong encryption or anonymity, to protect their privacy?

5.4 Spam

5.4.1 What's the Problem?

Defining spam is not a simple task, especially if one is defining it in a law to restrict it. Most, but not all, spam is commercial advertising.

Spam angers people because of both the content and the way it is sent. Many people just do not want any unsolicited ads and announcements. ISPs filter out e-mail from known spammers, so some disguise their return address and use other schemes to avoid filters.

Why is spam a problem? "Junk mail" is one form of violation of privacy: unwanted intrusion. The recipient has the annoyance of receiving junk mail, wasting time reading enough to determine what it is, and deleting it.

Spam costs service providers who need a system large and fast enough to handle the load and who must deal with the clog of undeliverable mail.

5.4.2 Cases and Free Speech Issues

AOL VERSUS CYBER PROMOTIONS AND OTHER SPAMMERS

In 1996, about half of the e-mail received at AOL was spam, and a lot of it came from a company called Cyber Promotions, an e-mail advertising service.

AOL installed filters to block mail from Cyber Promotions. Cyber Promotions changed its return address to avoid the filters and obtained an injunction against AOL's use of filters, claiming its First Amendment rights were being violated. Thus began the battle over the legal status of spam.

AOL's property rights allow it to decide what it accepts on its system. AOL is a membership organization; it can implement policies to provide the kind of environment it believes its members want. AOL is a private company, not a government institution.

Cyber Promotions sought an injunction to stop AOL from filtering out its e-mail. AOL sought injunctions to stop spammers from sending e-mail.

Do any of arguments support injunctions against the spammers? One does: the argument that the spam uses the recipient company's property against its wishes and imposes a cost on the recipient. AOL and other services won multimillion-dollar settlements from Cyber Promotions and other spammers.

INTEL EMPLOYEE

A former Intel employee, Ken Hamidi, sent six mass e-mailings to more than 30,000 Intel employees. Intel sought a court order prohibiting him from sending more e-mail to its employees (at work). Should the judge have granted the order? Would it infringe Hamidi's freedom of speech? Intel argued that freedom of speech did not give him the right to intrude in Intel's property and use its equipment to deliver his messages. The judge granted the order.

5.4.3 Solutions

MARKETS, TECHNOLOGY, AND BUSINESS POLICY

ISPs can block certain e-mail from their systems entirely and also let individual members establish their own lists and criteria for mail to block.

How much discretion should an anti-spam listing service have in deciding whom to include on its list of spammers?

Spam is cheap

ANTI-SPAM LAWS

Several anti-spam laws have been introduced in Congress, but none had passed by the time this book was written.

A key problem with any government actions, injunctions, or laws to restrict or prohibit spam is that they might conflict with freedom of speech.

Provisions in proposed laws include the following:

- Unsolicited commercial e-mail must be labeled so that it can easily be filtered out.
- ISPs must provide filters for members to block spam.
- Spam must identify the sender and include instructions for opting out.
- Senders must honor opt-out requests from recipients and send them no additional mail.
- Spam must include a valid e-mail reply address.
- False or misleading subject lines are prohibited.
- All unsolicited commercial e-mail is banned.

More than a dozen states have laws regulating spam sent to people in the state.

It is not always feasible to determine the location of the recipient.

The globalness of the Net adds another problem; if laws are passed in one country, but not in most others, many spammers will set up shop on computers outside the country.

5.5 Ensuring Valuable and Diverse Content

Computer Professionals for Social Responsible (CPSR); Lawrence Grossman, former president of the Public Broadcasting System (PBS) and NBC News; and philosophers who write about computer ethics, advocate a variety of legal regulations, taxes and subsidies, and other mechanisms to ensure that content they consider desirable is available on the Web.

It is worth examining the arguments for subsidizing or requiring certain content that some people deem desirable and not sufficiently available.

CPSR suggested the establishment of “public spaces” on the Net.

The purpose is to provide both access to information and a place for anyone to post messages with a guarantee of freedom of speech.

Subsidized programs might promote particular political, social, or aesthetic views that some taxpayers oppose; a freedom-of-speech issue arises whenever governments subsidize content. Also, opponents view subsidies and regulations as unnecessary, given the extraordinary variety on the Web.

EXPERIENCES WITH OTHER INFORMATION MEDIA

There are many parallels between the Internet and publishing.

The development of enormous diversity of information and opinion on the Web has been similar, though enormously quicker.

No one publisher or one consumer decides what will or will not be published.

Television and radio have been more regulated and less diverse than print media.

What could prevent diversity of content on the Web from continuing? With mergers between large companies like AOL and Time Warner, there is still concern that, as large news and entertainment conglomerates move into cyberspace, only a few points of view will be presented.