# Blown to Bits

## *Your Life, Liberty, and Happiness After the Digital Explosion*

Hal Abelson
Ken Ledeen
Harry Lewis

Addison-Wesley

Upper Saddle River, NJ • Boston • Indianapolis • San Francisco
New York • Toronto • Montreal • London • Munich • Paris • Madrid
Cape Town • Sydney • Tokyo • Singapore • Mexico City

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the publisher was aware of a trademark claim, the designations have been printed with initial capital letters or in all capitals.

The authors and publisher have taken care in the preparation of this book, but make no expressed or implied warranty of any kind and assume no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or programs contained herein.

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact:

U.S. Corporate and Government Sales
(800) 382-3419
corpsales@pearsontechgroup.com

For sales outside the United States, please contact:

International Sales
international@pearson.com

Visit us on the Web: www.informit.com/aw

*Library of Congress Cataloging-in-Publication Data:*

Abelson, Harold.
Blown to bits : your life, liberty, and happiness after the digital explosion / Hal Abelson, Ken Ledeen, Harry Lewis.
p. cm.
ISBN 0-13-713559-9 (hardback : alk. paper) 1. Computers and civilization. 2. Information technology—Technological innovations. 3. Digital media. I. Ledeen, Ken, 1946- II. Lewis, Harry R. III. Title.
QA76.9.C66A245 2008
303.48'33—dc22

2008005910



For information regarding permissions, write to:

Pearson Education, Inc.
Rights and Contracts Department
501 Boylston Street, Suite 900
Boston, MA 02116
Fax (617) 671 3447

ISBN-13: 978-0-13-713559-2
ISBN-10: 0-13-713559-9
Text printed in the United States on recycled paper at RR Donnelley in Crawfordsville, Indiana.
Third printing December 2008

**This Book Is Safari Enabled**

The Safari® Enabled icon on the cover of your favorite technology book means the book is available through Safari Bookshelf. When you buy this book, you get free access to the online edition for 45 days.

Safari Bookshelf is an electronic reference library that lets you easily search thousands of technical books, find code samples, download chapters, and access technical information whenever and wherever you need it.

To gain 45-day Safari Enabled access to this book:

- Go to http://www.informit.com/onlineedition
- Complete the brief registration form
- Enter the coupon code 9SD6-IQLD-ZDNI-AGEC-AG6L

If you have difficulty registering on Safari Bookshelf or accessing the online edition, please e-mail customer-service@safaribooksonline.com.

**Editor in Chief**
Mark Taub

**Acquisitions Editor**
Greg Doench

**Development Editor**
Michael Thurston

**Managing Editor**
Gina Kanouse

**Senior Project Editor**
Kristy Hart

**Copy Editor**
Water Crest Publishing, Inc.

**Indexer**
Erika Millen

**Proofreader**
Williams Woods Publishing Services

**Publishing Coordinator**
Michelle Housley

**Interior Designer and Composition**
Nonie Ratcliff

**Cover Designer**
Chuti Prasertsith

CHAPTER 7

# You Can't Say That on the Internet

## *Guarding the Frontiers of Digital Expression*

## Do You Know Where Your Child Is on the Web Tonight?

It was every parent's worst nightmare. Katherine Lester, a 16-year-old honors student from Fairgrove, Michigan, went missing in June 2006. Her parents had no idea what had happened to her; she had never given them a moment's worry. They called the police. Then federal authorities got involved.

After three days of terrifying absence, she was found, safe—in Amman, Jordan.

Fairgrove is too small to have a post office, and the Lesters lived in the last house on a dead-end street. In another time, Katherine's school, six miles away, might have been the outer limit of her universe. But through the Internet, her universe was—the whole world. Katherine met a Palestinian man, Abdullah Jimzawi, from Jericho on the West Bank. She found his profile on the social networking web site, MySpace, and sent him a message: "u r cute." They quickly learned everything about each other through online messages. Lester tricked her mother into getting her a passport, and then took off for the Middle East. When U.S. authorities met her plane in Amman, she agreed to return home, and apologized to her parents for the distress she had caused them.

A month later, Representative Judy Biggert of Illinois rose in the House to co-sponsor the Deleting Online Predators Act (DOPA). "MySpace.com and

other networking web sites have become new hunting grounds for child predators," she said, noting that "we were all horrified" by the story of Katherine Lester. "At least let's give parents some comfort that their children won't fall prey while using the Internet at schools and libraries that receive federal funding for Internet services." The law would require those institutions to prevent children from using on-location computers to access chat rooms and social networking web sites without adult supervision.

Speaker after speaker rose in the House to stress the importance of protecting children from online predators, but not all supported the bill. The language was "overbroad and ambiguous," said one. As originally drafted, it seemed to cover not just MySpace, but sites such as Amazon and Wikipedia. These sites possess some of the same characteristics as MySpace—users can create personal profiles and continually share information with each other using the Web. Although the law might block children in schools and libraries from "places" where they meet friends (and sometimes predators), it would also prevent access to online encyclopedias and bookstores, which rely on content posted by users.

Instead of taking the time to develop a sharper definition of what exactly was to be prohibited, DOPA's sponsors hastily redrafted the law to omit the definition, leaving it to the Federal Communications Commission to decide later just what the law would cover. Some murmured that the upcoming midterm elections were motivating the sponsors to put forward an ill-considered and showy effort to protect children—an effort that would likely be ineffective and so vague as to be unconstitutional.

Children use computers in lots of places; restricting what happens in schools and libraries would hardly discourage determined teenagers from sneaking onto MySpace. Only the most overbearing parents could honestly answer the question *USA Today* asked in its article about "cyber-predators": "It's 11 p.m. Do you know where your child is on the Web tonight?"

The statistics about what can go wrong were surely terrifying. The Justice Department has made thousands of arrests for "cyber enticement"—almost always older men using social networking web sites to lure teenagers into meetings, some of which end very badly. Yet, as the American Library Association stated in opposition to DOPA, education, not prohibition, is the "key to safe use of the Internet." Students have to learn to cooperate online, because network use, and all the human interactions it enables, are basic tools of the new, globally interconnected world of business, education, and citizenship.

And perhaps even the globally interconnected world of true love. The tale of Katherine Lester took an unexpected turn. From the moment she was found in Jordan, Lester steadily insisted that she intended to marry Jimzawi.

Jimzawi, who was 20 when he and Lester first made contact, claimed to be in love with her—and his mother agreed. Jimzawi begged Lester to tell her parents the truth before she headed off to meet him, but she refused. Upon her return, authorities charged Lester as a runaway child and took her passport away from her. But on September 12, 2007, having attained legal independence by turning 18, she again boarded a plane to the Middle East, finally to meet her beloved face to face. The affair finally ended a few weeks later in an exchange of accusations and denials, and a hint that a third party had attracted Lester's attentions. There was no high-tech drama to the breakup—except that it was televised on *Dr. Phil*.

The explosion in digital communications has confounded long-held assumptions about human relationships—how people meet, how they come to know each other, and how they decide if they can trust each other. At the same time, the explosion in digital information, in the form of web pages and downloadable photographs, has put at the fingertips of millions material that only a few years ago no one could have found without great effort and expense. Political dissidents in Chinese Internet cafés can (if they dare) read pro-democracy blogs. People all around the world who are ashamed about their illness, starved for information about their sexual identity, or eager to connect with others of their minority faith can find facts, opinion, advice, and companionship. And children too small to leave home by themselves can see lurid pornography on their families' home computers. Can societies anymore control what their members see and to whom they talk?

## Metaphors for Something Unlike Anything Else

DOPA, which has not been passed into law, is the latest battle in a long war between conflicting values. On the one hand, society has an interest in keeping unwanted information away from children. On the other hand, society as a whole has an interest in maximizing open communication. The U.S. Constitution largely protects the freedom to speak and the right to hear. Over and over, society has struggled to find a metaphor for electronic communication that captures the ways in which it is the same as the media of the past and the ways in which it is different. Laws and regulations are built on traditions; only by understanding the analogies can the speech principles of the past be extended to the changed circumstances of the present—or be consciously transcended.

What laws should apply? The Internet is not exactly like anything else. If you put up a web site, that is something like publishing a book, so perhaps

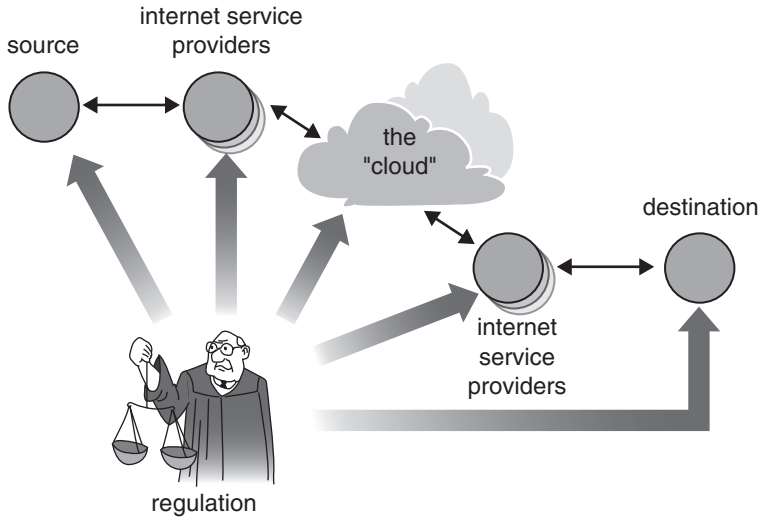
the laws about books should apply. But that was Web 1.0—a way for "publishers" to publish and viewers to view. In the dynamic and participatory Web 2.0, sites such as MySpace change constantly in response to user postings. If you send an email, or contribute to a blog, that is something like placing a telephone call, or maybe a conference call, so maybe laws about telephones should be the starting point. Neither metaphor is perfect. Maybe television is a better analogy, since browsing the Web is like channel surfing—except that the Internet is two-way, and there is no limit to the number of "channels."

Underneath the web software and the email software is the Internet itself. The Internet just delivers packets of bits, not knowing or caring whether they are parts of books, movies, text messages, or voices, nor whether the bits will wind up in a web browser, a telephone, or a movie projector. John Perry Barlow, former lyricist for the Grateful Dead and co-founder of the Electronic Frontier Foundation, used a striking metaphor to describe the Internet as it burst into public consciousness in the mid-1990s. The world's regulation of the flow of information, he said, had long controlled the transport of wine bottles. In "meatspace," the physical world, different rules applied to books, postal mail, radio broadcasts, and telephone calls—different kinds of bottles. Now the wine itself flowed freely through the network, nothing but bits freed from their packaging. Anything could be put in, and the same kind of thing would come out. But in between, it was all the same stuff—just bits. What are the rules of Cyberspace—what are the rules for the bits themselves?

When information is transmitted between two parties, whether the information is spoken words, written words, pictures, or movies, there is a source and a destination. There may also be some intermediaries. In a lecture hall, the listeners hear the speaker directly, although whoever provided the hall also played an important role in making the communication possible. Books have authors and readers, but also publishers and booksellers in between. It is natural to ascribe similar roles to the various parties in an Internet communication, and, when things go wrong, to hold any and all of the parties responsible. For example, when Pete Solis contacted a 14-year-old girl ("Jane Doe") through her MySpace profile and allegedly sexually assaulted her when they met in person, the girl's parents sued MySpace for $30 million for enabling the assault.

The Internet has a complex structure. The source and destination may be friends emailing each other, they may be a commercial web site and a residential customer, or they may be one office of a company sending a mockup of an advertising brochure to another office halfway around the world. The source and destination each has an ISP. Connecting the ISPs are routing switches, fiber optic cables, satellite links, and so on. A packet that flows through the Internet may pass through devices and communication links

owned by dozens of different parties. For convenience (and in the style of Jonathan Zittrain), we'll call the collection of devices that connect the ISPs to each other *the cloud*. As shown in Figure 7.1, speech on the Internet goes from the source to an ISP, into the cloud, out of the cloud to another ISP, and to its destination (see the sidebar, "Cloud Computing," in Chapter 3 for additional information about this).




Based on figure by Jonathan Zittrain

FIGURE 7.1 Where to regulate the Internet?

If a government seeks to control speech, it can attack at several different points. It can try to control the speaker or the speaker's ISP, by criminalizing certain kinds of speech. But that won't work if the speaker isn't in the same country as the listener. It can try to control the listener, by prohibiting possession of certain kinds of materials. In the U.S., possession of copyrighted software without an appropriate license is illegal, as is possession of other copyrighted material with the intent to profit from redistributing it. If citizens have reasonable privacy rights, however, it is hard for the government to know what its citizens possess. In a society such as the U.S., where citizens have reasonable rights of due process, one-at-a-time prosecutions for possession are unwieldy. As a final alternative, the government can try to control the intermediaries.

There are parallels in civil law. The parents of the Jane Doe sued MySpace because it was in the communication path between Mr. Solis and their daughter, even though MySpace was not the alleged assailant.

**Defaming Public Figures**

Damaging statements about public figures, even if false, are not defamatory unless they were made with malicious intent. This extra clause protects news media against libel claims by celebrities who are offended by the way the press depicts them. It was not always so, however. The pivotal case was *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964), in which the newspaper was sued by officials in Alabama on the basis of a pro-civil-rights advertisement it published. The story is detailed, along with a readable history of the First Amendment, in *Make No Law* by Anthony Lewis (Vintage Paperback, 1992). For a later account of First Amendment struggles, see Lewis's *Freedom for the Thought That We Hate* (Basic Books, 2008).

Very early, defamation laws had to adapt to the Internet. In the U.S., speech is defamatory if it is false, communicated to third parties, and damages one's reputation.

In the physical world, when the speaker defames someone, the intermediaries between the speaker and the listener sometimes share responsibility with the speaker—and sometimes not. If we defame someone in this book, we may be sued, but so may the book's publisher, who might have known that what we were writing was false. On the other hand, the trucker who transported the book to the bookstore probably isn't liable, even though he too helped get our words from us to our readers. Are the various electronic intermediaries more like publishers, or truckers? Do the parents of Jane Doe have a case against MySpace?

Society has struggled to identify the right metaphors to describe the parties to an electronic communication. To understand this part of the story of electronic information, we have to go back to pre-Internet electronic communication.

## Publisher or Distributor?

CompuServe was an early provider of computer services, including bulletin boards and other electronic communities users could join for a fee. One of these fora, Rumorville USA, provided a daily newsletter of reports about broadcast journalism and journalists. CompuServe didn't screen or even collect the rumors posted on Rumorville. It contracted with a third party, Don Fitzpatrick Associates (DFA), to provide the content. CompuServe simply posted whatever DFA provided without reviewing it. And for a long time, no one complained.

In 1990, a company called Cubby, Inc. started a competing service, Skuttlebut, which also reported gossip about TV and radio broadcasting. Items appeared on Rumorville describing Skuttlebut as a "new start-up scam" and alleging that its material was being stolen from Rumorville. Cubby cried foul and went after CompuServe, claiming defamation. CompuServe acknowledged that the postings were defamatory, but claimed it was not acting as a publisher of the information—just a distributor. It simply was sending on to subscribers what other people gave it. It wasn't responsible for the contents, any more than a trucker is responsible for libel that might appear in the magazines he handles.

What was the right analogy? Was CompuServe more like a newspaper, or more like the trucker who transports the newspaper to its readers?

More like the trucker, ruled the court. A long legal tradition held distributors blameless for the content of the publications they delivered. Distributors can't be expected to have read all the books on their trucks. Grasping for a better analogy, the court described CompuServe as "an electronic for-profit library." Distributor or library, CompuServe was independent of DFA and couldn't be held responsible for libelous statements in what DFA provided. The case of *Cubby v. CompuServe* was settled decisively in CompuServe's favor. Cubby might go after the source, but that wasn't CompuServe. CompuServe was a blameless intermediary. So was MySpace, years later, when Jane Doe's parents sought redress for Mr. Solis's alleged assault of their daughter. In a ruling building on the *Cubby* decision, MySpace was absolved of responsibility for what Solis had posted.

When *Cubby v. CompuServe* was decided, providers of computer services everywhere exhaled. If the decision had gone the other way, electronic distribution of information might have become a risky business that few dared to enter. Computer networks created an information infrastructure unprecedented in its low overhead. A few people could connect tens of thousands, even millions, to each other at very low cost. If everything disseminated had to be reviewed by human readers before it was posted, to ensure that any damaging statements were truthful, its potential use for participatory democracy would be severely limited. For a time, a spirit of freedom ruled.

## Neither Liberty nor Security

"The law often demands that we sacrifice some liberty for greater security. Sometimes, though, it takes away our liberty to provide us less security." So wrote law professor Eugene Volokh in the fall of 1995, commenting on a court case that looked similar to *Cubby v. CompuServe*, but wasn't.

Eugene Volokh has a blog, `volokh.com`, in which he comments regularly on information freedom issues and many other things.

Prodigy was a provider of computer services, much like CompuServe. But in the early 1990s, as worries began to rise about the sexual content of materials available online, Prodigy sought to distinguish itself as a family-oriented service. It pledged to exercise editorial control over the postings on its bulletin boards. "We make no apology," Prodigy stated, "for pursuing a value system that reflects the culture of the millions of American families we aspire to serve. Certainly no responsible newspaper does less...." Prodigy's success in the market was due in no small measure to the security families felt in accessing its fora, rather than the anything-goes sites offered by other services.

One of Prodigy's bulletin boards, called "Money Talk," was devoted to financial services. In October 1994, someone anonymously posted comments on Money Talk about the securities investment firm Stratton Oakmont. The firm, said the unidentified poster, was involved in "major criminal fraud." Its president was "soon to be proven criminal." The whole company was a "cult of brokers who either lie for a living or get fired."

Stratton Oakmont sued Prodigy for libel, claiming that Prodigy should be regarded as the publisher of these defamatory comments. It asked for $200 million in damages. Prodigy countered that it had zero responsibility for what its posters said. The matter had been settled several years earlier by the *Cubby v. CompuServe* decision. Prodigy wasn't the publisher of the comments, just the distributor.

In a decision that stunned the Internet community, a New York court ruled otherwise. By exercising editorial control in support of its family-friendly image, said the court, Prodigy became a publisher, with the attendant responsibilities and risks. Indeed, Prodigy had likened itself to a newspaper publisher, and could not at trial claim to be something less.

It was all quite logical, as long as the choice was between two metaphors: distributor or newspaper. In reality, though, a service provider wasn't exactly like either. Monitoring for bad language was a pretty minor form of editorial work. That was a far cry from checking everything for truthfulness.

Be that as it may, the court's finding undercut efforts to create safe districts in Cyberspace. After the decision, the obvious advice went out to bulletin board operators: Don't even consider editing or censoring. If you do, *Stratton Oakmont v. Prodigy* means you may be legally liable for any malicious falsehood that slips by your review. If you don't even try, *Cubby v. CompuServe* means you are completely immune from liability.

This was fine for the safety of the site operators, but what about the public interest? Freedom of expression was threatened, since fewer families would be willing to roam freely through the smut that would be posted. At the same time, security would not be improved, since defamers could always post their lies on the remaining services with their all-welcome policies.

## The Nastiest Place on Earth

Every communication technology has been used to control, as well as to facilitate, the flow of ideas. Barely a century after the publication of the Gutenberg Bible, Pope Paul IV issued a list of 500 banned authors. In the United States, the First Amendment protects authors and speakers from government interference: *Congress shall make no law ... abridging the freedom of speech, or of the press* .... But First Amendment protections are not absolute. No one has the right to publish obscene materials. The government can destroy materials it judges to be obscene, as postal authorities did in 1918 when they burned magazines containing excerpts of James Joyce's *Ulysses*.

What exactly counts as obscene has been a matter of much legal wrangling over the course of U.S. history. The prevailing standard today is the one the Supreme Court used in 1973 in deciding the case of *Miller v. California*, and is therefore called the *Miller Test*. To determine whether material is obscene, a court must consider the following:

1. Whether the average person, applying contemporary community standards, would find that the work, taken as a whole, appeals to the prurient interest.
2. Whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law.
3. Whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.

Only if the answer to each part is "yes" does the work qualify as obscene. The Miller decision was a landmark, because it established that there were no national standards for obscenity. There were only "community" standards, which could be different in Mississippi than in New York City. But there were no computer networks in 1973. What is a "community" in Cyberspace?

*What is a "community" in Cyberspace?*

In 1992, the infant World Wide Web was hardly world-wide, but many Americans were using dial-up connections to access information on centralized, electronic bulletin boards. Some bulletin boards were free and united communities of interest—lovers of baseball or birds, for example. Others distributed free software. Bob and Carleen Thomas of Milpitas, California, ran a different kind of bulletin board, called Amateur Action. In their advertising, they described it as "The Nastiest Place on Earth."

For a fee, anyone could download images from Amateur Action. The pictures were of a kind not usually shown in polite company, but readily available in magazines sold in the nearby cities of San Francisco and San Jose. The Thomases were raided by the San Jose police, who thought they might have been distributing obscene materials. After looking at their pictures, the police decided that the images were not obscene by local standards.

Bob and Carleen were not indicted, and they added this notice to their bulletin board: "The San Jose Police Department as well as the Santa Clara County District Attorney's Office and the State of California agree that Amateur Action BBS is operating in a legal manner."

Two years later, in February 1994, the Thomases were raided again, and their computer was seized. This time, the complaint came from Agent David Dirmeyer, a postal inspector—in *western Tennessee*. Using an assumed name, Dirmeyer had paid $55 and had downloaded images to his computer in Memphis. Nasty stuff indeed, particularly for Memphis: bestiality, incest, and sado-masochism. The Thomases were arrested. They stood trial in Memphis on federal charges of transporting obscene material via common carrier, and via interstate commerce. They were convicted by a Tennessee jury, which concluded that their Milpitas bulletin board violated the community standards of Memphis. Bob was sentenced to 37 months incarceration and Carleen to 30.

The Thomases appealed their conviction, on the grounds that they could not have known where the bits were going, and that the relevant community, if not San Jose, was a community of Cyberspace. The appeals court did not agree. Dirmeyer had supplied a Tennessee postal address when he applied for membership in Amateur Action. The Thomases had called him at his Memphis telephone number to give him the password—they had known where he was. The Thomases, concluded the court, should have been more careful where they sent their bits, once they started selling them out of state. Shipping the bits was just like shipping a videotape by UPS (a charge of which the Thomases were also convicted). The laws of meatspace applied to Cyberspace—and one city's legal standards sometimes applied thousands of miles away.

## The Most Participatory Form of Mass Speech

Pornography was part of the electronic world from the moment it was possible to store and transmit words and images. The Thomases learned that bits were like books, and the same obscenity standards applied.

In the mid-1990s, something else happened. The spread of computers and networks vastly increased the number of digital images available and the number of people viewing them. Digital pornography became not just the same old thing in a new form—it seemed to be a brand-new thing, because there was so much of it and it was so easy to get in the privacy of the home. Nebraska Senator James Exon attached an anti-Internet-pornography amendment to a telecommunications bill, but it seemed destined for defeat on civil liberties grounds. And then all hell broke loose.

On July 3, 1995, *Time Magazine* blasted "CYBERPORN" across its cover. The accompanying story, based largely a single university report, stated:

> *What the Carnegie Mellon researchers discovered was: THERE'S AN AWFUL LOT OF PORN ONLINE. In an 18-month study, the team surveyed 917,410 sexually explicit pictures, descriptions, short stories, and film clips. On those Usenet newsgroups where digitized images are stored, 83.5% of the pictures were pornographic.*

The article later noted that this statistic referred to only a small fraction of all data traffic, but failed to explain that the offending images were mostly on limited-access bulletin boards, not openly available to children or anyone else. It mentioned the issue of government censorship, and it quoted John Perry Barlow on the critical role of parents. Nonetheless, when Senator Grassley of Iowa read the *Time Magazine* story into the Congressional Record, attributing its conclusions to a study by the well-respected Georgetown University Law School, he called on Congress to "help parents who are under assault in this day and age" and to "help stem this growing tide."

Grassley's speech, and the circulation in the Capitol building of dirty pictures downloaded by a friend of Senator Exon, galvanized the Congress to save the children of America. In February 1996, the Communications Decency Act, or CDA, passed almost unanimously and was signed into law by President Clinton.

The CDA made it a crime to use "any interactive computer service to display in a manner available to a person 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." Criminal penalties would also fall on anyone who "knowingly permits any telecommunications facility under such person's control to be used" for such prohibited activities. And finally, it criminalized the transmission of materials that were "obscene or indecent" to persons known to be under 18.

These "display provisions" of the CDA vastly extended existing anti-obscenity laws, which already applied to the Internet. The dual prohibitions against *making offensive images available to a person under 18*, and against transmitting *indecent materials to persons known to be under 18*, were unlike anything that applied to print publications. "Indecency," whatever it meant, was something short of obscenity, and only obscene materials had been illegal prior to the CDA. A newsstand could tell the difference between a 12-year-old customer and a 20-year-old, but how could anyone check ages in Cyberspace?

When the CDA was enacted, John Perry Barlow saw the potential of the Internet for the free flow of information challenged. He issued a now-classic manifesto against the government's effort to regulate speech:

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You have no sovereignty where we gather.... We are creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth. We are creating a world where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity.... In our world, all the sentiments and expressions of humanity, from the debasing to the angelic, are parts of a seamless whole, the global conversation of bits.... [Y]ou are trying to ward off the virus of liberty by erecting guard posts at the frontiers of Cyberspace.

Brave and stirring words, even if the notion of Cyberspace as a "seamless whole" had already been rendered doubtful. At a minimum, bits had to meet different obscenity standards in Memphis than in Milpitas, as the Thomases

had learned. In fact, the entire metaphor of the Internet as a "space" with "frontiers" was fatally flawed, and misuse of that metaphor continues to plague laws and policies to this day.

Civil libertarians joined the chorus challenging the Communications Decency Act. In short order, a federal court and the U.S. Supreme Court ruled in the momentous case of *ACLU v. Reno*. The display provisions of the CDA were unconstitutional. "The Government may only regulate free speech for a compelling reason," wrote Judge Dalzell in the district court decision, "and in the least restrictive manner." It would chill discourse unacceptably to demand age verification over the Internet from every person who might see material that any adult has a legal right to see.

The government had argued that the authority of the Federal Communications Commission (FCC) to regulate the content of TV and radio broadcasts, which are required not to be "indecent," provided an analogy for government oversight of Internet communications.

The courts disagreed. The FCC analogy was wrong, they ruled, because the Internet was far more open than broadcast media. Different media required different kinds of laws, and the TV and radio laws were more restrictive than laws were for print media, or should be for the Internet. "I have no doubt" wrote Judge Dalzell, "that a Newspaper Decency Act, passed because Congress discovered that young girls had read a front page article in the *New York Times* on female genital mutilation in Africa, would be unconstitutional.... The Internet may fairly be regarded as a never-ending worldwide conversation. The Government may not, through the CDA, interrupt that conversation. As the most participatory form of mass speech yet developed, the Internet deserves the highest protection from governmental intrusion." The CDA's display provisions were dead.

In essence, the court was unwilling to risk the entire Internet's promise as a vigorous marketplace of ideas to serve the narrow purpose of protecting children from indecency. Instead, it transferred the burden of blocking unwanted communications from source ISPs to the destination. The DOPA's proposed burden on libraries and schools is heir to the court's ruling overturning the CDA. Legally, there seemed to be nowhere else to control speech except at the point where it came out of the cloud and was delivered to the listener.

Lost in the 1995–96 Internet indecency hysteria was the fact that the "Carnegie Mellon report" that started the legislative ball rolling had been discredited almost as soon as the *Time Magazine* story appeared. The report's author, Martin Rimm, was an Electrical Engineering undergraduate. His

**Defending Electronic Freedoms**

The Electronic Frontier Foundation, `www.eff.org`, is the leading public advocacy group defending First Amendment and other personal rights in Cyberspace. Ironically, it often finds itself in opposition with media and telecommunications companies. In principle, communications companies should have the greatest interest in unfettered exchange of information. In actual practice, they often benefit financially from policies that limit consumer choice or expand surveillance and data-gathering about private citizens. The EFF was among the plaintiffs bringing suit in the case that overturned the CDA.

study's methodology was flawed, and perhaps fraudulent. For example, he told adult bulletin board operators that he was studying how best to market pornography online, and that he would repay them for their cooperation by sharing his tips. His conclusions were unreliable. Why hadn't that been caught when his article was published? Because the article was not a product of Georgetown University, as Senator Grassley had said. Rather, it appeared in the *Georgetown Law Review*, a student publication that used neither peer nor professional reviewers. Three weeks after publishing the "Cyberporn" article, *Time* acknowledged that Rimm's study was untrustworthy. In spite of this repudiation, Rimm salvaged something from his efforts: He published a book called *The Pornographer's Handbook: How to Exploit Women, Dupe Men, & Make Lots of Money.*

## Protecting Good Samaritans—and a Few Bad Ones

The *Stratton Oakmont v. Prodigy* decision, which discouraged ISPs from exercising any editorial judgment, had been handed down in 1995, just as Congress was preparing to enact the Communications Decency Act to protect children from Internet porn. Congress recognized that the consequences of *Stratton Oakmont* would be fewer voluntary efforts by ISPs to screen their sites for offensive content. So, the bill's sponsors added a "Good Samaritan" provision to the CDA.

The intent was to allow ISPs to act as editors without running the risk that they would be held responsible for the edited content, thus putting themselves in the jam in which Prodigy had found itself. So the CDA included a provision absolving ISPs of liability on account of anything they did, in good faith,

to filter out "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable" material. For good measure, the CDA pushed the *Cubby* court's "distributor" metaphor to the limit, and beyond. ISPs should *not* be thought of as publishers, or as sources either. "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." This was the bottom line of §230 of the CDA, and it meant that there would be no more *Stratton Oakmont v. Prodigy* Catch-22s.

When the U.S. Supreme Court struck down the CDA in 1996, it negated only the display provisions, the clauses that threatened the providers of "indecent" content. The Good Samaritan clause was allowed to stand and remains the law today. ISPs can do as much as they want to filter or censor their content, without any risk that they will assume publishers' liabilities in the process.

Or as little as they choose, as Ken Zeran learned to his sorrow a few years later.

### The CDA and Discrimination

The "Good Samaritan" clause envisioned a sharp line between "service providers" (which got immunity) and "content providers" (which did not). But as the technology world evolved, the distinction became fuzzy. A roommate-matching service was sued in California, on the basis that it invited users to discriminate by categorizing their roommate preferences (women only, for example). A court ruled that the operators of the web site were immune as service providers. An appeals court reversed the decision, on the basis that the web site became a content provider by filtering the information applicants provided—people seeking female roommates would not learn about men looking for roommates. There was nothing wrong with *that*, but the principle that the roommate service had *blanket* protection, under the CDA, to filter as it wished would mean that with equal impunity, it could ask about racial preferences and honor them. That form of discrimination would be illegal in newspaper ads. "We doubt," wrote the appeals court judge, "this is what Congress had in mind when it passed the CDA."

The worst terrorist attack in history on U.S. soil prior to the 2001 destruction of New York's World Trade Center was the bombing of the Alfred P. Murrah Federal building in Oklahoma City on April 19, 1995. 168 people were killed, some of them children in a day care center. Hundreds more were injured when the building collapsed around them and glass and rubble rained down on the neighborhood. One man who made it out alive likened the event to the detonation of an atomic bomb.

Less than a week later, someone with screen name "Ken ZZ03" posted an advertisement on an America On Line (AOL) bulletin board. Ken had "Naughty Oklahoma T-Shirts" for sale. Among the available slogans were "Visit Oklahoma—it's a Blast" and "Rack'em, Stack'em, and Pack'em—Oklahoma 1995." Others were even cruder and more tasteless. To get your T-shirt, said the ads, you should call Ken. The posting gave Ken's phone number.

The number belonged to Ken Zeran, an artist and filmmaker in Seattle, Washington. Zeran had nothing to do with the posting on AOL. It was a hoax.

Ken Zeran started to receive calls. Angry, insulting calls. Then death threats.

Zeran called AOL and asked them to take down the posting and issue a retraction. An AOL employee promised to take down the original posting, but said retractions were against company policy.

The next day, an anonymous poster with a slightly different screen name offered more T-shirts for sale, with even more offensive slogans.

*Call Ken*. And by the way—there's high demand. So if the phone is busy, call back.

Zeran kept calling AOL to ask that the postings be removed and that further postings be prevented. AOL kept promising to close down the accounts and remove the postings, but didn't. By April 30, Ken was receiving a phone call every two minutes. Ken's art business depended on that phone number—he couldn't change it or fail to answer it, without losing his livelihood.

About this time, Shannon Fullerton, the host of a morning drive-time radio talk show on KRXO in Seattle, received by email a copy of one of the postings. Usually his show was full of light-hearted foolishness, but after the bombing, Fullerton and his radio partner had devoted several shows to sharing community grief about the Oklahoma City tragedy. Fullerton read Ken's T-shirt slogans over the air. And he read Ken's telephone number and told his listeners to call Ken and tell him what they thought of him.

Zeran got even more calls, and more death threats. Fearing for his safety, he obtained police surveillance of his home. Most callers were not interested

in hearing what Ken had to say when he answered the phone, but he managed to keep one on the line long enough to learn about the KRXO broadcast. Zeran contacted the radio station. KRXO issued a retraction, after which the number of calls Ken received dropped to fifteen per day. Eventually, a newspaper exposed the hoax. AOL finally removed the postings, after leaving them visible for a week. Ken's life began to return to normal.

**WAS THE RADIO STATION LIABLE?**

Zeran sued the radio station separately, but failed in that effort as well. Much as he may have suffered, reasoned the court, it wasn't defamation, because none of the people who called him even knew who Ken Zeran was—so his reputation couldn't possibly have been damaged when the radio station spoke ill of "Ken"!

Zeran sued AOL, claiming defamation, among other things. By putting up the postings, and leaving them up long after it had been informed that they were false, AOL had damaged him severely.

The decision went against Zeran, and the lower court's decision held up on appeal. AOL certainly had behaved like a publisher, by communicating the postings in the first place and by choosing not to remove them when informed that they were fraudulent. Unlike the defendant in the *Cubby v. CompuServe* case, AOL knew exactly what it was publishing. But the Good Samaritan provision of the CDA specifically stated that AOL should not legally be *treated* as a publisher. AOL had no liability for Zeran's woes.

Zeran's only recourse was to identify the actual speaker, the pseudonymous Ken ZZ03 who made the postings. And AOL would not help him do that. Everyone felt sorry for Ken, but the system gave him no help.

The posters could evade responsibility as long as they remained anonymous, as they easily could on the Internet. And Congress had given the ISPs a complete waiver of responsibility for the consequences of false and damaging statements, even when the ISP knew they were false. Had anyone in Congress thought through the implications of the Good Samaritan clause?

## Laws of Unintended Consequences

The Good Samaritan provision of the CDA has been the friend of free speech, and a great relief to Internet Service Providers. Yet its application has defied logical connection to the spirit that created it.

Sidney Blumenthal was a Clinton aide whose job it was to dish dirt on the president's enemies. On August 11, 1997, conservative online columnist Matt Drudge reported, "Sidney Blumenthal has a spousal abuse past that has been effectively covered up." The White House denied it, and the next day Drudge withdrew the claim. The Blumenthals sued AOL, which had a deal with Drudge. And had deeper pockets—the Blumenthals asked for $630,000,021. AOL was as responsible for the libel as Drudge, claimed the Blumenthals, because AOL could edit what Drudge supplied. AOL could even insist that Drudge delete items AOL did not want posted. The court sided with AOL, and cited the Good Samaritan clause of the CDA. AOL couldn't be treated like a publisher, so it couldn't be held liable for Drudge's falsehoods. Case closed.

*The Communications Decency Act has been used to protect an ISP whose chat room was being used to peddle child pornography.*

Even more strangely, the Good Samaritan clause of the Communications Decency Act has been used to protect an ISP whose chat room was being used to peddle child pornography.

In 1998, Jane and John Doe, a mother and her minor son, sued AOL for harm inflicted on the son. The Does alleged that AOL chat rooms were used to sell pornographic images of the boy made when he was 11 years old. They claimed that in 1997, Richard Lee Russell had lured John and two other boys to engage in sexual activities with each other and with Russell. Russell then used AOL chat rooms to market photographs and videotapes of these sexual encounters.

Jane Doe complained to AOL. Under the terms of its agreement with its users, AOL specifically reserved the right to terminate the service of anyone engaged in such improper activities. And yet AOL did not suspend Russell's service, or even warn him to stop what he was doing. The Does wanted compensation from AOL for its role in John Doe's sexual abuse.

The Does lost. Citing the Good Samaritan clause, and the precedent of the *Zeran* decision, the Florida courts held AOL blameless. Online service providers who knowingly allow child pornography to be marketed on their bulletin boards could not be treated as though they had published ads for kiddie porn.

The Does appealed and lost again. The decision in AOL's favor was 4-3 at the Florida Supreme Court. Judge J. Lewis fairly exploded in his dissenting opinion. The Good Samaritan clause was an attempt to remove disincentives from the development of filtering and blocking technologies, which would assist parents in their efforts to protect children. "[I]t is inconceivable that Congress intended the CDA to shield from potential liability an ISP alleged to have taken absolutely no actions to curtail illicit activities ... while profiting

from its customer's continued use of the service." The law had been transformed into one "which both condones and exonerates a flagrant and reprehensible failure to act by an ISP in the face of ... material unquestionably harmful to children." This made no sense. The sequence of decisions "thrusts Congress into the unlikely position of having enacted legislation that encourages and protects the involvement of ISPs as silent partners in criminal enterprises for profit."

The problem, as Judge Lewis saw it, was that it wasn't enough to say that ISPs were not like publishers. They really were more like distributors—as Ken Zeran had tried to argue—and distributors are not *entirely* without responsibility for what they distribute. A trucker who knows he is carrying child pornography, and is getting a cut of the profits, has *some* legal liability for his complicity in illegal commerce. His role is not that of a publisher, but it is not nothing either. The *Zeran* court had created a muddle by using the wrong analogy. Congress had made the muddle possible by saying nothing about the right analogy after saying that publishing was the wrong one.

## Can the Internet Be Like a Magazine Store?

After the display provision of the CDA was ruled unconstitutional in 1997, Congress went back to work to protect America's children. The Child Online Protection Act (COPA), passed into law in 1998, contained many of the key elements of the CDA, but sought to avoid the CDA's constitutional problems by narrowing it. It applied only to "commercial" speech, and criminalized knowingly making available to minors "material harmful to minors." For the purposes of this law, a "minor" was anyone under 17. The statute extended the Miller Test for obscenity to create a definition of material that was not obscene but was "harmful to minors:"

> The term "material that is harmful to minors" means any communication ... that – (A) the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to ... the prurient interest; (B) depicts, describes, or represents, in a manner patently offensive with respect to minors, ... [a] sexual act, or a lewd exhibition of the genitals or post-pubescent female breast; and (C) taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.

COPA was challenged immediately and never took effect. A federal judge enjoined the government from enforcing it, ruling that it was likely to be unconstitutional. The matter bounced between courts through two presidencies. The case started out as *ACLU v. Reno*, for a time was known as *ACLU v. Ashcroft*, and was decided as *ACLU v. Gonzalez*. The judges were uniformly sympathetic to the intent of Congress to protect children from material they should not see. But in March 2007, the ax finally fell on COPA. Judge Lowell A. Reed, Jr., of U.S. District Court for the Eastern District of Pennsylvania, confirmed that the law went too far in restricting speech.

Part of the problem was with the vague definition of material "harmful to minors." The prurient interests of a 16-year-old were not the same as those of an 8-year-old; and what had literary value for a teenager might be valueless for a younger child. How would a web site designer know which standard he should use to avoid the risk of imprisonment?

But there was an even more basic problem. COPA was all about keeping away from minors material that would be perfectly legal for adults to have. It put a burden on information distributors to ensure that recipients of such information were of age. COPA provided a "safe harbor" against prosecution for those who in good faith checked the ages of their customers. Congress imagined a magazine store where the clerks wouldn't sell dirty magazines to children who could not reach the countertop, and might ask for identification of any who appeared to be of borderline age. The law envisioned that something similar would happen in Cyberspace:

> It is an affirmative defense to prosecution under this section that the defendant, in good faith, has restricted access by minors to material that is harmful to minors (A) by requiring use of a credit card, debit account, adult access code, or adult personal identification number; (B) by accepting a digital certificate that verifies age; or (C) by any other reasonable measures that are feasible under available technology.

The big problem was that these methods either didn't work or didn't even exist. Not every adult has a credit card, and credit card companies don't want their databases used to check customers' ages. And if you don't know what is meant by an "adult personal identification number" or a "digital certificate that verifies age," don't feel badly—neither do we. Clauses (B) and (C) were basically a plea from Congress for the industry to come up with some technical magic for determining age at a distance.

In the state of the art, however, computers can't reliably tell if the party on the other end of a communications link is human or is another computer. For a computer to tell whether a human is over or under the age of 17, even imperfectly, would be very hard indeed. Mischievous 15-year-olds could get around any simple screening system that could be used in the home. The Internet just isn't like a magazine store.

Even if credit card numbers or personal identification systems could distinguish children from adults, Judge Reed reasoned, such methods would intimidate computer users. Fearful of identity theft or government surveillance, many computer users would refuse interrogation and would not reveal personal identifying information as the price for visiting web sites deemed "harmful to minors." The vast electronic library would, in practice, fall into disuse and start to close down, just as an ordinary library would become useless if everyone venturing beyond the children's section had to endure a background check.

Congress's safe harbor recommendations, concluded Judge Reed, if they worked at all, would limit Internet speech drastically. Information adults had a right to see would, realistically, become unavailable to them. The filtering technologies noted when the CDA was struck down had improved, so the government could not credibly claim that limiting speech was the only possible approach to protecting children. And even if the free expression concerns were calmed or ignored, and even if everything COPA suggested worked perfectly, plenty of smut would still be available to children. The Internet was borderless, and COPA's reach ended at the U.S. frontier. COPA couldn't stop the flood of harmful bits from abroad.

Summing up, Reed quoted the thoughts of Supreme Court Justice Kennedy about a flag-burning case. "The hard fact is that sometimes we must make decisions we do not like. We make them because they are right, right in the sense that the law and the Constitution, as we see them, compel the result." Much as he was sympathetic to the end of protecting children from harmful communications, Judge Reed concluded, "perhaps we do the minors of this country harm if First Amendment protections, which they will with age inherit fully, are chipped away in the name of their protection."

## Let Your Fingers Do the Stalking

Newsgroups for sharing sexual information and experiences started in the early 1980s. By the mid-90s, there were specialty sites for every orientation and inclination. So when a 28-year-old woman entered an Internet chat room

in 1998 to share her sexual fantasies, she was doing nothing out of the ordinary. She longed to be assaulted, she said, and invited men reading her email to make her fantasy a reality. "I want you to break down my door and rape me," she wrote.

What *was* unusual was that she gave her name and address—and instructions about how to get past her building's security system. Over a period of several weeks, nine men took up her invitation and showed up at her door, often in the middle of the night. When she sent them away, she followed up with a further email to the chat room, explaining that her rejections were just part of the fantasy.

In fact, the "woman" sending the emails was Gary Dellapenta, a 50-year-old security guard whose attentions the actual woman had rebuffed. The victim of this terrifying hoax did not even own a computer. Dellapenta was caught because he responded directly to emails sent to entrap him. He was convicted and imprisoned under a recently enacted California anti-"cyberstalking" statute. The case was notable not because the events were unusual, but because it resulted in a prosecution and conviction. Most victims are not so successful in seeking redress. Most states lacked appropriate laws, and most victims could not identify their stalkers. Sometimes the stalker did not even know the victim—but simply found her contact information somewhere in Cyberspace.

Speeches and publications with frightening messages have long received First Amendment protections in the U.S., especially when their subject is political. Only when a message is likely to incite "imminent lawless action" (in the words of a 1969 Supreme Court decision) does speech become illegal—a test rarely met by printed words. This high threshold for government intervention builds on a "clear and present danger" standard explained most eloquently by Justice Louis Brandeis in a 1927 opinion. "Fear of serious injury cannot alone justify suppression of free speech .... No danger flowing from speech can be deemed clear and present, unless the incidence of the evil apprehended is so imminent that it may befall before there is opportunity for full discussion."

Courts apply the same standard to web sites. An anti-abortion group listed the names, addresses, and license plate numbers of doctors performing abortions on a web site called the "Nuremberg Files." It suggested stalking the doctors, and updated the site by graying out the names of those who had been wounded and crossing off those who had been murdered. The web site's creators acknowledged that abortion was legal, and claimed not to be threatening anyone, only collecting dossiers in the hope that the doctors could at some point in the future be held accountable for "crimes against humanity."

The anti-abortion group was taken to court in a civil action. After a long legal process, the group was found liable for damages because "true threats of violence were made with the intent to intimidate."

The courts had a very difficult time with the question of whether the Nuremberg Files web site was threatening or not, but there was nothing intrinsic to the mode of publication that complicated that decision. In fact, the same group had issued paper "WANTED" posters, which were equally part of the materials at issue. Reasonable jurists could, and did, come to different conclusions about whether the text on the Nuremberg Files web site met the judicial threshold.

But the situation of Dellapenta's victim, and other women in similar situations, seemed to be different. The scores being settled at their expense had no political dimensions. There were already laws against stalking and telephone harassment; the Internet was being used to recruit proxy stalkers and harassers. Following the lead of California and other states, Congress passed a federal anti-cyberstalking law.

## Like an Annoying Telephone Call?

The "2005 Violence Against Women and Department of Justice Reauthorization Act" (signed into law in early 2006) assigned criminal penalties to anyone who "utilizes any device or software that can be used to originate telecommunications or other types of communications that are transmitted, in whole or in part, by the Internet ... without disclosing his identity and with intent to annoy, abuse, threaten, or harass any person...." The clause was little noticed when the Act was passed in the House on a voice vote and in the Senate unanimously.

Civil libertarians again howled, this time about a single word in the legislation. It was fine to outlaw abuse, threats, and harassment by Internet. Those terms had some legal history. Although it was not always easy to tell whether the facts fit the definitions, at least the courts had standards for judging what these words meant.

But "annoy"? People put lots of annoying things on web sites and say lots of annoying things in chat rooms. There is even a web site, `annoy.com`, devoted to posting annoying political messages anonymously. Could Congress really have intended to ban the use of the Internet to annoy people?

Congress had extended telephone law to the Internet, on the principle that harassing VoIP calls should not receive more protection than harassing landline telephone calls. In using broad language for electronic communications,

however, it created another in the series of legal muddles about the aptness of a metaphor.

The Telecommunications Act of 1934 made it a criminal offense for anyone to make "a telephone call, whether or not conversation ensues, without disclosing his identity and with intent to annoy, abuse, threaten, or harass any person at the called number." In the world of telephones, the ban posed no threat to free speech, because a telephone call is one-to-one communication. If the person you are talking to doesn't want to listen, your free speech rights are not infringed. The First Amendment gives you no right to be sure anyone in particular hears you. If your phone call is unwelcome, you can easily find another forum in which to be annoying. The CDA, in a clause that was not struck down along with the display provisions, extended the prohibition to faxes and emails—still, basically, person-to-person communications. But harassing VoIP calls were not criminal under the Telecommunications Act. In an effort to capture all telephone-like technologies under the same regulation, the same clause was extended to all forms of electronic communication, including the vast "electronic library" and "most participatory form of mass speech" that is the Internet.

Defenders of the law assured alarmed bloggers that "annoying" sites would not be prosecuted unless they also were personally threatening, abusive, or harassing. This was an anti-cyberstalking provision, they argued, not a censorship law. Speech protected by the First Amendment would certainly be safe. Online publishers, on the other hand, were reluctant to trust prosecutors' judgment about where the broadly written statute would be applied. And based on the bizarre and unexpected uses to which the CDA's Good Samaritan provisions had been put, there was little reason for confidence that the legislative context for the law would restrict its application to one corner of Cyberspace.

The law was challenged by The Suggestion Box, which describes itself as helping people send anonymous emails for reasons such as to "report sensitive information to the media" and to "send crime tips to law enforcement agencies anonymously." The law, as the complaint argued, might criminalize the sort of employee whistle-blowing that Congress encouraged in the aftermath of scandals about corporate accounting practices. The Suggestion Box dropped its challenge when the Government stated that mere annoyances would not be prosecuted, only communications meant "to instill fear in the victim." So the law is in force, with many left wishing that Congress would be more precise with its language!

Which brings us to the present. The "annoyance" clause of the Violence Against Women Act stands, but only because the Government says that it doesn't mean what it says. DOPA, with which this chapter began, remains

stuck in Congress. Like the CDA and COPA, DOPA has worthy goals. The measures it proposes would, however, probably do more harm than good. In requiring libraries to monitor the computer use of children using sites such as MySpace, it would likely make those sites inaccessible through public libraries, while having little impact on child predators. The congressional sponsors have succumbed to a well-intentioned but misguided urge to control a social problem by restricting the technology that assists it.

## Digital Protection, Digital Censorship—and Self-Censorship

The First Amendment's ban on government censorship complicates government efforts to protect the safety and security of U.S. citizens. Given a choice between protection from personal harm and some fool's need to spout profanities, most of us would opt for safety. Security is immediate and freedom is long-term, and most people are short-range thinkers. And most people think of security as a personal thing, and gladly leave it to the government to worry about the survival of the nation.

*Given a choice between protection from personal harm and some fool's need to spout profanities, most of us would opt for safety.*

But in the words of one scholar, the bottom line on the First Amendment is that "in a society pledged to self-government, it is never true that, in the long run, the security of the nation is endangered by the freedom of the people." The Internet censorship bills have passed Congress by wide margins because members of Congress dare not be on record as voting against the safety of their constituents—and especially against the safety of children. Relatively isolated from political pressure, the courts have repeatedly undone speech-restricting legislation passed by elected officials.

Free speech precedes the other freedoms enumerated in the Bill of Rights, but not just numerically. In a sense, it precedes them logically as well. In the words of Supreme Court Justice Benjamin Cardozo, it is "the matrix, the indispensable condition, of nearly every other form of freedom."

For most governments, the misgivings about censoring electronic information are less profound.

In Saudi Arabia, you can't get to `www.sex.com`. In fact, *every* web access in Saudi Arabia goes through government computers to make sure the URL isn't

**INTERNET FREEDOM**

A great many organizations devote significant effort to maintaining the Internet's potential as a free marketplace of ideas. In addition to EFF, already mentioned earlier in this chapter, some others include: the Electronic Privacy Information Network, `www.epic.org`; The Free Expression Network, `freeexpression.org`, which is actually a coalition; the American Civil Liberties Union, `www.aclu.org`; and the Chilling Effects Clearinghouse, `www.chillingeffects.org`. The OpenNet Initiative, `opennet.net`, monitors Internet censorship around the world. OpenNet's findings are presented in *Access Denied: The Practice and Policy of Global Internet Filtering*, by Ronald J. Deibert, John G. Palfrey, Rafal Rohozinski, and Jonathan Zittrain (eds.), MIT Press, 2008.

on the government's blacklist. In Thailand, `www.stayinvisible.com` is blocked; that's a source of information about Internet privacy and tools to assist in anonymous web surfing.

The disparity of information freedom standards between the U.S. and other countries creates conflicts when electronic transactions involve two nations. As discussed in Chapter 4, China insists that Google not help its citizens get information the government does not want them to have. If you try to get to certain web sites from your hotel room in Shanghai, you suddenly lose your Internet connection, with no explanation. You might think there was a glitch in the network somewhere, except that you can reconnect and visit other sites with no problems.

Self-censorship by Internet companies is also increasing—the price they pay for doing business in certain countries. Thailand and Turkey blocked the video-sharing site YouTube after it carried clips lampooning (and, as those governments saw it, insulting) their current or former rulers. A Google official described censorship as the company's "No. 1 barrier to trade." Stirred by the potential costs in lost business and legal battles, Internet companies have become outspoken information libertarians, even as they do what must be done to meet the requirements of foreign governments. Google has even hired a Washington lobbyist to seek help from the U.S. government in its efforts to resist censorship abroad.

It is easy for Americans to shrug their isolationist shoulders over such problems. As long as all the information is available in the U.S., one might reason, who cares what version of Google or YouTube runs in totalitarian regimes abroad? That is for those countries to sort out.

But the free flow of information into the U.S. is threatened by the laws of other nations about the operation of the press. Consider the case of Joseph Gutnick and *Barron's* magazine.

On October 30, 2000, the financial weekly *Barron's* published an article suggesting that Australian businessman Joseph Gutnick was involved in money-laundering and tax evasion. Gutnick sued Dow Jones Co., the publisher of *Barron's*, for defamation. The suit was filed in an Australian court. Gutnick maintained that the online edition of the magazine, available in Australia for a fee, was in effect published in Australia. Dow Jones countered that the place of "publication" of the online magazine was New Jersey, where its web servers were located. The suit, it argued, should have been brought in a U.S. court and judged by the standards of U.S. libel law, which are far more favorable to the free speech rights of the press. The Australian court agreed with Gutnick, and the suit went forward. Gutnick ultimately won an apology from Dow Jones and $580,000 in fines and legal costs.

The implications seem staggering. Americans on American soil expect to be able to speak very freely, but the Australian court claimed that the global Internet made Australia's laws applicable wherever the bits reaching Australian soil may have originated. The Amateur Action conundrum about what community standards apply to the borderless Internet had been translated to the world of global journalism. Will the freedom of the Internet press henceforth be the minimum applying to any of the nations of the earth? Is it possible that a rogue nation could cripple the global Internet press by extorting large sums of money from alleged defamers, or by imposing death sentences on reporters it claimed had insulted their leaders?

The American press tends to fight hard for its right to publish the truth, but the censorship problems reach into Western democracies more insidiously for global corporations not in the news business. It is sometimes easier for American companies to meet the minimum "world" standards of information freedom than to keep different information available in the U.S. There may even be reasons in international law and trade agreements that make such accommodations to censorship more likely. Consider the trials of Yahoo! France.

In May 2000, the League Against Racism and Anti-Semitism (LICRA, in its French acronym) and the Union of French Jewish Students (UEJF) demanded to a French court that Yahoo! stop making Nazi paraphernalia available for online auction, stop showing pictures of Nazi memorabilia, and prohibit the dissemination of anti-Semitic hate speech on discussion groups available in France. Pursuant to the laws of France, where the sale and display of Nazi items is illegal, the court concluded that what Yahoo! was doing was an

offense to the "collective memory" of the country and a violation of Article R654 of the Penal Code. It told Yahoo! that the company was a threat to "internal public order" and that it had to make sure no one in France could view such items.

Yahoo! removed the items from the `yahoo.fr` site ordinarily available in France. LICRA and UEJF then discovered that from within France, they could also get to the American site, `yahoo.com`, by slightly indirect means. Reaching across the ocean in a manner reminiscent of the Australian court's defamation action, the French court demanded that the offending items, images, and words be removed from the American web site as well.

Yahoo! resisted for a time, claiming it couldn't tell where the bits were going—an assertion somewhat lacking in credibility since the company tended to attach French-language advertising to web pages if they were dispatched to locations in France. Eventually, Yahoo! made a drastic revision of its standards for the U.S. site. Hate speech was prohibited under Yahoo's revised service terms with its users, and most of the Nazi memorabilia disappeared. But Nazi stamps and coins were still available for auction on the U.S. site, as were copies of *Mein Kampf*. In November 2000, the French court affirmed and extended its order: *Mein Kampf* could not be offered for sale in France. The fines were adding up.

Yahoo! sought help in U.S. courts. It had committed no crime in the U.S., it stated. French law could not leap the Atlantic and trump U.S. First Amendment protections. Enforcement of the French order would have a chilling effect on speech in the United States. A U.S. district court agreed, and the decision was upheld on appeal by a three-judge panel of the Court of Appeals for the Ninth Circuit (Northern California).

But in 2006, the full 11-member court of appeals reversed the decision and found against Yahoo!. The company had not suffered enough, according to the majority opinion, nor tried long enough to have the French change their minds, for appeal to First Amendment protections to be appropriate. A dissenting opinion spoke plainly about what the court seemed to be doing. "We should not allow a foreign court order," wrote Judge William Fletcher, "to be used as leverage to quash constitutionally protected speech...."

*It would be a sad irony if information liberty, so stoutly defended for centuries in the U.S., would fall in the twenty-first century to a combination of domestic child protection laws and international money-making opportunities.*

Such conflicts will be more common in the future, as more bits flow

across national borders. The laws, trade agreements, and court decisions of the next few years, many of them regulating the flow of "intellectual property," will shape the world of the future. It would be a sad irony if information liberty, so stoutly defended for centuries in the U.S., would fall in the twenty-first century to a combination of domestic child protection laws and international money-making opportunities. But as one British commentator said when the photo-hosting site Flickr removed photos to conform with orders from Singapore, Germany, Hong Kong, and Korea, "Libertarianism is all very well when you're a hacker. But business is business."

Information freedom on the Internet is a tricky business. Technological changes happen faster than legal changes. When a technology shift alarms the populace, legislators respond with overly broad laws. By the time challenges have worked their way through the courts, another cycle of technology changes has happened, and the slow heartbeat of lawmaking pumps out another poorly drafted statute.

The technology of radio and television has also challenged the legislative process, but in a different way. In the broadcast world, strong commercial forces are arrayed in support of speech-restricting laws that have long since outgrown the technology that gave birth to them. We now turn to those changes in the radio world.