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.