3

Freedom of Speech

3.1 Communications Paradigms

> *Congress shall make no law . . . abridging the freedom of speech, or of the press. . . .*
>
> —First Amendment, U.S. Constitution

As we observed in Chapter 1, the Internet brought us extraordinary opportunities for increasing free expression of ideas, easy and inexpensive communication between people of different countries, and extraordinary opportunities for access to many voices and points of view all over the world. But freedom of speech has always been restricted to some degree in the United States and to a large degree in many other countries. In this chapter, we examine how principles of freedom of speech from earlier media affect the Internet and how the Internet affects them.* We consider pornography on the Internet, attempts to restrict it, and attempts to restrict access by children; advertising and commerce on the Web; spam (mass, unsolicited email); and anonymity as a protection for speakers. Some forms of speech have long been contentious (pornography, for example), and some are new forms that developed with the Internet and other digital technology (spam and video games, for example). When the First Amendment protects some forms of controversial speech (such as violent video games or leaking sensitive documents) from legal restrictions, ethical and social issues are particularly relevant. Throughout this chapter, we describe various incidents and cases and discuss issues they raise. In Section 3.5, we examine how communications and surveillance technologies affect freedom of speech in different countries, especially some that have a long tradition of censorship.

3.1.1 Regulating Communications Media

It is by now almost a cliché to say that the Internet lets us all be publishers. We do not need expensive printing presses or complex distribution systems. We need only a computer or a cellphone. Any business, organization, or individual can set up a website. We can "publish" whatever we wish; it is available for anyone who chooses to read it. In 1994, shortly before the Web became widely used, Mike Godwin, then an attorney with the Electronic Frontier Foundation, described the dramatic change that computer communications brought about:

> It is a medium far different from the telephone, which is only a one-to-one medium, ill-suited for reaching large numbers of people. It is a medium far different from the newspaper or TV station, which are one-to-many media, ill-suited for feedback from the audience. For the first time in history, we have a many-to-many medium,

* Although some of our discussion is in the context of the U.S. Constitution's First Amendment, the arguments and principles about the human right of freedom of speech apply globally.

> in which you don't have to be rich to have access, and in which you don't have to win the approval of an editor or publisher to speak your mind. Usenet* and the Internet, as part of this new medium, hold the promise of guaranteeing, for the first time in history, that the First Amendment's protection of freedom of the press means as much to each individual as it does to Time Warner, or to Gannett, or to the *New York Times*.[1]

Individuals took advantage of that promise. As just one indication, the number of blogs passed 150 million by 2010.[2] Some are as widely read and as influential as traditional newspapers. However, while computer communications technologies *might* guarantee freedom of speech and of the press for all of us, the guarantee is not certain.

Telephone, movies, radio, television, cable, satellites, and, of course, the Internet did not exist when the Constitution was written. Freedom of the press applied to publishers who printed newspapers and books and to "the lonely pamphleteer" who printed and distributed pamphlets expressing unconventional ideas. One might think the First Amendment should apply to each new communications technology according to its spirit and intention: to protect our freedom to say what we wish. Politically powerful people, however, continually try to restrict speech that threatens them. From the Alien and Sedition Acts of 1798 to regulation of Political Action Committees, such laws have been used against newspaper editors who disagreed with the political party in power and against ad hoc groups of people speaking out on issues. Attempts to restrict freedom of speech and of the press flourish with new technologies. Law professor Eric M. Freedman sums up: "Historical experience—with the printing press, secular dramatic troupes, photographs, movies, rock music, broadcasting, sexually explicit telephone services, video games, and other media—shows that each new medium is viewed at first by governments as uniquely threatening, because it is uniquely influential, and therefore a uniquely appropriate target of censorship."[3]

In this section, we introduce the traditional three-part framework for First Amendment protection and government regulation of communications media that developed in the United States in the 20th century. As we will see, modern communications technology and the Internet required that the framework be updated. The three categories are:

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

The first category has the strongest First Amendment protection. Although books have been banned in the United States and people were arrested for publishing information on certain topics such as contraception, the trend has been toward fewer government restraints on the printed word.

---

* An early (pre-Web) collection of Internet discussion groups.

Television and radio are similar to newspapers in their role of providing news and entertainment, but the government regulates both the structure of the broadcasting industry and the content of programs. The government grants broadcasting licenses. Licensees must meet government standards of merit—a requirement that would not be tolerated for publishers because of the obvious threat to freedom of expression. The government has used threats of license revocation to get stations to cancel sexually oriented talk shows or to censor them. Since 1971, the government has banned cigarette ads from radio, television, and electronic media under the control of the Federal Communications Commission (FCC), but the ads continued to be legal in magazines and newspapers. In a 1978 case challenging the constitutionality of a ban on broadcast "indecency," the Supreme Court upheld the ban.* The federal government frequently proposes requirements to reduce violence on television or increase programming for children, but the government cannot impose such requirements on print publishers. Whether you favor or oppose particular regulations, the point is that the government has more control over television and radio content than it has over communication methods that existed at the time the Bill of Rights was written. The main argument used to deny full First Amendment protection to broadcasters was scarcity of broadcast frequencies. There were only a handful of television channels and few radio frequencies in the early days of broadcasting. In exchange for the "monopoly" privilege of using the scarce, publicly owned spectrum, broadcasters were tightly regulated. With cable, satellites, hundreds of channels, and competition from the Internet, the argument based on scarcity and monopoly is irrelevant now, but the precedent of government control remains. A second argument, still used to justify government-imposed restrictions on content, is that broadcast material comes into the home and is difficult to keep from children.

Common carriers provide a medium of communication (not content) and must make their service available to everyone. In some cases, as with telephone service, the government requires them to provide "universal access" (i.e., to subsidize service for people with low incomes). Based on the argument that common carriers are a monopoly, the law prohibited them from controlling the content of material that passes through their system. Telephone companies were prohibited from providing content or information services on the grounds that they might discriminate against competing content providers who must also use their telephone lines. Common carriers had no control over content, so they had no responsibility for illegal content passing through.

Beginning in the 1980s, computer bulletin board systems (BBS), commercial services like CompuServe, Prodigy, and America Online (AOL), and ultimately the World Wide Web became major arenas for distribution of news, information, and opinion. Because of the immense flexibility of computer communications systems, they do not fit neatly into the publishing, broadcasting, and common carriage paradigms. Cable television strained these categories previously. In commenting on a law requiring cable stations to carry

* The FCC had fined comedian George Carlin for a radio program about the seven dirty words one could not say on the radio.

certain broadcasts, the Supreme Court said cable operators have more freedom of speech than television and radio broadcasters, but less than print publishers.[4] But the Web does not fit between the existing categories any better than it fits within any one of them. It has similarities to all three, as well as additional similarities to bookstores, libraries, and rented meeting rooms—all of which the law treats differently.

As new technologies blurred the technical boundaries between cable, telephone, computer networks, and content providers, the law began to adapt. The Telecommunications Act of 1996 changed the regulatory structure. It removed many artificial legal divisions of service areas and many restrictions on services that telecommunications companies may provide. It also significantly clarified the question of the liability of Internet Service Providers (ISPs) and other online service providers for content posted by third parties such as members and subscribers. Print publishers and broadcasters are legally liable for content they publish or broadcast. They can be sued for libel (making false and damaging statements) and copyright infringement, for example. They are legally responsible for obscene material in their publications and programs. Before passage of the Telecommunications Act, several people brought suits against BBS operators, ISPs, AOL, and other service providers for content that others put on their systems. To protect themselves from lawsuits and possible criminal charges, service providers would likely have erred on the side of caution and removed much content that was legal—seriously restricting the amount of information and opinion in cyberspace. The Telecommunications Act stated that "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."[5] This statement removed uncertainty and protected service providers, thus encouraging the growth of user-created content.*

In 1996, the main parts of the first major Internet censorship law, the Communications Decency Act, were ruled unconstitutional. However, efforts to censor the Internet continued. We investigate arguments about, as well as the impacts of, censorship and other restrictive laws in Section 3.2. In addition, we will see in Section 3.2.5 that many innovative individuals and entrepreneurs who tried to publish information, advertise products, and provide services on the Web encountered legal problems (and sometimes fines), not because of explicit censorship laws, but because of long-standing laws that restricted commerce to benefit powerful organizations, businesses, and governments. In several cases, these confrontations between new technology and old laws resulted in increased freedom.

3.1.2 Free Speech Principles

As we proceed with our discussion of free speech issues, it is helpful to remember several important points.

---

* Service providers remain at risk in many countries. For example, the head of eBay in India was arrested because someone sold pornographic videos on eBay's Indian site even though the video itself did not appear on the site and the seller violated company policy by selling them.

The First Amendment was written precisely for offensive and/or controversial speech and ideas. There is no need to protect speech and publication that no one objects to. The First Amendment covers spoken and written words, pictures, art, and other forms of expression of ideas and opinions.

The First Amendment is a restriction on the power of government, not individuals or private businesses. Publishers do not have to publish material they consider offensive, poorly written, or unlikely to appeal to their customers for any reason. Rejection or editing by a publisher is not a violation of a writer's First Amendment rights. Websites, search engine companies, and magazines may decline specific advertisements if they so choose. That does not violate the advertiser's freedom of speech.

Over the course of many years and many cases, the Supreme Court has developed principles and guidelines about protected expression.* When a government action or law causes people to avoid legal speech and publication out of fear of prosecution—perhaps because a law is vague—the action or law is said to have a "chilling effect" on First Amendment rights. Courts generally rule that laws with a significant chilling effect are unconstitutional. Advocating illegal acts is (usually) legal; a listener has the opportunity and responsibility to weigh the arguments and decide whether or not to commit the illegal act. The First Amendment does not protect libel and direct, specific threats. Inciting violence, in certain circumstances, is illegal. Although the First Amendment makes no distinctions among categories of speech, courts have treated advertising as "second class" speech and allowed restrictions that would not be acceptable for other kinds of speech. However, cases in recent years have gone against that trend. Courts have begun to rule that restrictions on truthful advertising do indeed violate the First Amendment.[6] Similarly, since the 1970s, the government has severely regulated political campaign speech, but recent Supreme Court decisions have restored some First Amendment protection for it. Many court decisions have protected anonymous speech, but there are serious attempts to limit or prohibit anonymity on the Internet.

There is a censorship issue whenever the government owns or substantially subsidizes communications systems or networks (or controversial services). For example, in the 1980s, federally subsidized family planning clinics were not permitted to discuss abortion. In the past, the government has made it illegal to send information through the mail that the First Amendment otherwise protects. A federal agency that provides funds for public radio stations rejected the application of a university because it broadcasts one hour a week of religious programming. In Section 3.2.2, we will see that Congress used its funding power to require censorship of the Internet in public libraries and schools. No matter what side of these issues you are on, no matter how the policy changes with different presidents or Congresses, the point is that, in many circumstances, when the government pays, it can choose to restrict speech that the Constitution would otherwise protect.

---

* The specific laws, court decisions, and guidelines are complex in some cases. The discussion here is general and simplified.

3.2 Controlling Speech

> *I disapprove of what you say, but I will defend to the death your right to say it.*
>
> —Voltaire's biographer, S. G. Tallentyre (Evelyn Beatrice Hall), describing Voltaire's view of freedom of speech[7]

3.2.1 Offensive Speech: What Is It? What Is Illegal?

What is offensive speech? What should the law prohibit or restrict on the Web? The answers depend on who you are. It could be political or religious speech, pornography, racial or sexual slurs, Nazi materials, libelous statements, abortion information, antiabortion information, advertising of alcoholic beverages, advertising in general, depictions of violence, discussion of suicide, or information about how to build bombs. There are vehement advocates for banning each of these—and more. The state of Georgia tried to ban pictures of marijuana from the Internet. A doctor argued for regulating medical discussion on the Net so that people would not get bad advice. The Chinese government restricts reporting of emergencies (such as major accidents or disasters) and how the government handles them. The French government approved a law banning anyone except professional journalists from recording or distributing video of acts of violence.

Most efforts to censor the Internet in the United States, including several laws passed by Congress, focus on pornographic and other sexually explicit material, so we use pornography as the first example. Many of the same principles apply to efforts to censor other kinds of material. People discuss sexual activity, of conventional and unconventional sorts, including pedophilia, in graphic detail in cyberspace. The distinctions between categories such as erotica, art, and pornography are not always clear, and different people have very different personal standards. There is much on the Net that is extremely offensive to adults. Some people want to prohibit it altogether. Some seek ways to keep it away from children.

The Internet began as a forum for research and scientific discussion, so the rapid proliferation of pornography shocked some people. It is not, however, a surprising development. The same kind of material was already available in adult magazines, bookstores, and movie theaters. As a writer for *Wired* contends, sexual material quickly invades all new technologies and art forms.[8] He points out that, from cave paintings to frescos in Pompeii to stone carvings at Angkor Wat, erotica have flourished. The printing press produced Bibles and porn. Photography produced *Playboy*. Many of the first videocassettes were pornographic. Hundreds of thousands of subscription websites provide adult entertainment.[9] Whether all this is good or bad—whether it is a natural part of human nature or a sign of degeneracy and evil, whether we should tolerate it or stamp it out—are moral and social issues beyond the scope of this book. People debate pornography endlessly.

In addressing the issue of pornography and of other kinds of speech that offend people, we try to focus specifically on new problems and issues related to computer systems and cyberspace.

What was already illegal?

In 1973, the Supreme Court, in *Miller v. California*, established a three-part guideline for determining whether material is obscene under the law. The First Amendment does not protect obscene material. The criteria are that (1) it depicts sexual (or excretory) acts whose depiction is specifically prohibited by state law, (2) it depicts these acts in a patently offensive manner, appealing to prurient interest as judged by a reasonable person using community standards, and (3) it has no serious literary, artistic, social, political, or scientific value. The second point—the application of community standards—was a compromise intended to avoid the problem of setting a national standard of obscenity in so large and diverse a country. Thus, small conservative or religious towns could restrict pornography to a greater extent than cosmopolitan urban areas.

It has long been illegal to create, possess, or distribute child pornography. We discuss child pornography further in Section 3.2.3, where we consider unexpected applications of the laws.

Straining old legal standards

On the Internet, communities have no physical locations. Instead, they are defined by the people who choose to associate in cyberspace because of common interests. The definition of "community" proved critical in an early Internet case. A couple in California operated a computer bulletin board system (BBS) called Amateur Action that made sexually explicit images available to members. Legal observers generally agreed that the Amateur Action BBS operators would not be found guilty of a crime in California. A postal inspector in Memphis, Tennessee, working with a U.S. attorney there, became a member of the BBS (the only member in Tennessee[10]) and downloaded sexually explicit images in Memphis. The couple, who lived and worked in California, were prosecuted in Tennessee and found guilty of distributing obscenity under the local community standards. Both received jail sentences. A spokesman for the American Civil Liberties Union (ACLU) commented that prosecutions like this one meant that "nothing can be put on the Internet that is more racy than would be tolerated in the most conservative community in the U.S."[11] For this reason, some courts have recognized that "community standards" is no longer an appropriate tool for determining what is acceptable material. (For different national standards, see Section 5.4.1.)

Different national standards: Section 5.4.1

The Net also changed the meaning of "distribution." Did the BBS operators send obscene files to Tennessee? BBSs were accessed through the telephone system. Anyone, from anywhere, could call in if they chose. The postal inspector in Tennessee initiated the telephone call to the BBS and initiated the transfer of the files. He selected and downloaded them. Critics of the prosecution of the BBS operators argued that it is as if the postal inspector went to California, bought pornographic pictures, and brought them home to Memphis—then had the seller prosecuted under Memphis community standards.[12]

3.2.2 Censorship Laws and Alternatives

Our sole intent is to make the Internet safer for our youth.

—Department of Justice spokesman[13]

Even where the protection of children is the object, the constitutional limits on government action apply.

—Justice Antonin Scalia[14]

Major Internet censorship laws

In the 1990s, as more nontechnical people began using the Internet, a variety of religious organizations, antipornography groups, and others began a campaign to pass federal legislation to censor the Internet. Increasing publicity about porn on the Net and increasing political pressure led Congress to pass the Communications Decency Act (CDA) of 1996.[15] In the CDA and the censorship laws that followed, Congress attempted to avoid an obvious conflict with the First Amendment by focusing on children. The CDA made it a crime to make available to anyone under 18 any communication that is obscene or indecent.

It can be difficult to design a law that keeps inappropriate material from children while allowing access for adults. The Supreme Court ruled on this problem in *Butler v. Michigan*, a significant 1957 case striking down a Michigan law that made it illegal to sell material that might be damaging to children. Justice Frankfurter wrote that the state must not "reduce the adult population of Michigan to reading only what is fit for children."[16] The CDA restricted indecent material accessible by children, but a child can access almost anything on the Net. Thus, opponents said, it would have violated Justice Frankfurter's dictum, not just in Michigan but throughout the country.

Opponents of the CDA gave examples of information that is legal in print but might be cause for prosecution if available online: the Bible, some of Shakespeare's plays, and serious discussions of sexual behavior and health problems like AIDS. Supporters of the CDA argued that this was overreaction. No one would be prosecuted, they said, for such material. The lack of clear standards, however, can lead to uneven and unfair prosecutions. The uncertainty about potential prosecution could have a chilling effect on those who provide information for adults that might not be suitable for children.

The Supreme Court ruled unanimously, in *American Civil Liberties Union et al. v. Janet Reno*, that the censorship provisions of the CDA were unconstitutional. The courts made strong statements about the importance of protecting freedom of expression in general and on the Internet. The decisions against the CDA established that "the Internet deserves the highest protection from government intrusion."

- Distinguish speech from action. Advocating illegal acts is (usually) legal.
- Laws must not chill expression of legal speech.
- Do not reduce adults to reading only what is fit for children.
- Solve speech problems by least restrictive means.

Figure 3.1 Freedom of speech guidelines.

Figure 3.1 summarizes principles courts use to help determine if a censorship law is constitutional. When the government is pursuing a legitimate goal that might infringe on free speech (in this case, the protection of children), it must use the least restrictive means of accomplishing the goal. The courts found that the then newly developing filtering software was less restrictive and more desirable than censorship. The judges also commented, "The government can continue to protect children from pornography on the Internet through vigorous enforcement of existing laws criminalizing obscenity and child pornography."[17]

Congress tried again, with the Child Online Protection Act (COPA), in 1998. This law was more limited than the CDA. COPA made it a federal crime for commercial websites to make available to minors material "harmful to minors" as judged by community standards. Once again, First Amendment supporters argued that the law was too broad and would threaten art, news, and health sites. Courts evaluating COPA noted that because the Web is accessible everywhere, the community-standards provision would restrict the entire country to the standards of the most conservative community. The courts said COPA restricts access to a substantial amount of online speech that is lawful for adults, and COPA's requirements that adults provide identification to view material not appropriate for minors would have an unconstitutional chilling effect on free speech. After more than 10 years of lawsuits and appeals, the Supreme Court declined to hear the last government appeal, and COPA died in 2009.

Congress passed the Children's Internet Protection Act (CIPA) in 2000 to require libraries and schools to use filter software on Internet terminals. When public libraries first installed Internet terminals, there were problems. People used the terminals to look at "X-rated" pictures, within view of children or other library users who found them offensive. Some people tied up terminals for hours viewing such material while others waited to use the terminals. Children accessed adult sexual material. Children and adults accessed extremist political sites and racist material. Librarians around the country tried to satisfy library users, parents, community organizations, civil libertarians, and their own Library Bill of Rights (which opposes restricting access to library materials because of age). Some installed polarizing filters on terminals or built walls around terminals so that the screens were visible only from directly in front (both to protect the privacy of

the user and to shield other users and employees from material they find objectionable). Most set time limits on use of terminals. Some librarians asked patrons to stop viewing pornography, just as they would ask someone to stop making noise. Some installed filtering software on all terminals, some on only terminals in the children's section. Some required parental supervision for children using the Internet, and some required written parental permission.

CIPA sought to override these methods. The authors of CIPA attempted to avoid the courts' objections to the CDA and COPA by using the federal government's funding power. CIPA requires that schools and libraries that participate in certain federal programs (receiving federal money for technology) install filtering software on all Internet terminals to block access to sites with child pornography, obscene material, and material "harmful to minors." Of course, many schools and libraries rely on those funds. Civil liberties organizations and the American Library Association sued to block CIPA.[18] The Supreme Court ruled that CIPA does not violate the First Amendment. CIPA does not require the use of filters. It does not impose jail or fines on people who provide content on the Internet. It sets a condition for receipt of certain federal funds. Courts often accept such conditions. The court made it clear that if an adult asks a librarian to disable the filter on a library Internet terminal the adult is using, the librarian must do so. Of course, some adults are unaware of the filter software, unaware that they can legally request it be turned off, or unwilling to call attention to themselves by making the request.

Outside of public schools and libraries, the trend of judicial decisions is to give the Internet First Amendment protection similar to that of print media, that is, the highest degree of protection.

Video games

Violent video games have been the focus of criticism since they began appearing. Some are very gory; some depict murder and torture; some focus on violence against women and members of specific ethnic and religious groups. Are they bad for children? Are they more dangerous than other forms of violence and violent sexism and racism that a minor sees in books or other media? Should we ban them?

Some argue that the interactivity of video games has a more powerful impact on children than passively watching television or reading a violent story. Others point out that children have played at killing each other (cops and robbers, cowboys and Indians) for generations. Does falling down "dead" on the grass compare to the repeated, explosive gore of a video game? At what age is a child mature enough to decide to play a violent video game: 12? 18? Who should decide what games a child plays: parents or legislators? Parents are not always with their children. They regularly worry that peer pressure overrides parental rules and guidance.

A California law banned sale or rental of violent video games to minors. In 2011, the Supreme Court ruled that the law violated the First Amendment. The Court pointed out

that violence and gore are common in classic fairy tales (for example, the grim Grimm Brothers), cartoons (Elmer Fudd always shooting at Bugs Bunny), superhero comics, and literature teenagers are required to read in high school. Many video games are extremely disgusting, but the Court said that "disgust is not a valid basis for restricting expression."[19] The Court considered research on the impact of video games on children's feelings of aggression and found that the impacts were small and differed little from the impacts of other media.

Alternatives to censorship

What alternatives to censorship are available to protect children from inappropriate material on the Net (and to shield adults from material that is offensive to them)? Are

Talking about bombs—or farming

Several terrorists who set off bombs in the United States and other countries researched bomb-making techniques on the Internet. Students who carried bombs into schools learned how to make them on the Internet. As far back as 1995, within a few weeks of the bombing of the Oklahoma City federal building, the Senate's terrorism and technology subcommittee held hearings on "The Availability of Bomb Making Information on the Internet." There are many similarities between the controversy about bomb-making information on the Net and the controversy about pornography. As with pornography, bomb-making information was already widely available in traditional media, protected by the First Amendment. It also has legitimate uses. Information about how to make bombs can be found in the print version of the *Encyclopedia Britannica* and in books in libraries and bookstores. The U.S. Department of Agriculture distributed a booklet called the "Blasters' Handbook"—farmers use explosives to remove tree stumps.[20]

Arguing to censor information about bombs on the Internet, Senator Dianne Feinstein said, "There is a difference between free speech and teaching someone to kill."[21] Arguing against censorship, a former U.S. attorney said that "information-plus," (i.e., information used in the commission of a criminal act) is what the law should regulate. Senator Patrick Leahy emphasized that it is "harmful and dangerous *conduct*, not speech, that justifies adverse legal consequences." This was already, in essence, established legal principle outside of cyberspace. There are, of course, existing laws against using bombs to kill people or destroy property, as well as laws against making bombs or conspiring to make them for such purposes.

Congress passed a law mandating 20 years in prison for anyone who distributes bomb-making information knowing or intending that it will be used to commit a crime. Although there have been several incidents since then in which people built and used bombs made with information from the Internet, no one has been tried under this law.[22] It is difficult to determine (and prove) what a person posting the information knows and intends about its uses.

there solutions that do not threaten to diminish free discussion of serious subjects or deny sexually explicit material to adults who want it? As we see for many problems, there are a variety of solutions based on the market, technology, responsibility, and education, as well as on enforcement of existing laws.

The development of software filters is an example of a quick market response to a problem. Many families with children use filtering software (some of which is free). Software filters work in a variety of ways. They can block websites with specific words, phrases, or images. They can block sites according to various rating systems. They can contain long lists of specific sites to block. Parents can choose categories to filter (e.g., sex or violence), add their own list of banned sites, and review a log their child's activity. But filters cannot do a perfect job. In fact, at first, many did a very poor job. They screened out both too much (sites about Middlesex and Essex) and too little (missing some obviously objectionable material). Filters blocked sites containing political discussion and educational material (for example, the home page of a university's biology department and the websites of a candidate for Congress containing statements about abortion and gun control). Filters improved with time, but it is not possible to completely eliminate errors and subjective views about what is too sexual or too violent or too critical of a religion, what medical information is appropriate for children of what age, what is acceptable to say about homosexuality, and so on. None of the solutions we describe in this book for problems generated by new technologies are perfect. They have strengths and weaknesses and are useful in some circumstances and not others. Parents can weigh pros and cons and make their choices. The weaknesses, however—particularly the blocking of legal material—do present a free speech issue when legislators mandate filters or when public institutions use filters.

Wireless carriers set strict "decency" standards for companies providing content for their networks. Their rules are detailed and stricter than what the government can prohibit.[23] Commercial services, online communities, and social networking sites develop policies to protect members. Methods include expelling subscribers who post or email material banned by law or the site's policies, removing offensive material, and aiding law enforcement with investigations of child pornography or attempts to meet and molest children. Social network sites developed technology to trace members who post child pornography. In response to market demand, companies offer online services, websites, and cellphone services targeted to families and children. Some allow subscribers to lock children out of certain areas. Parents can set up accounts without email for their children or set up a specified list of addresses from which their children's accounts can receive email. The video game industry developed a rating system that provides an indication for parents about the amount of sex, profanity, and violence in a game.[24] Some online game sites restrict their offerings to nonviolent games and advertise that policy. Many online services distribute information with tips on how to control what children view. The websites of the

FBI and organizations such as the National Center for Missing and Exploited Children[25] provide information about risks to children and guidelines for reducing them.

Parents have a responsibility to supervise their children and to teach them how to deal with inappropriate material and threats. But technology certainly has changed the risks to children and made the parents' job more difficult. If a young child tried to buy a ticket for an X-rated movie at a movie theater or to buy an adult magazine in a store, a cashier would see the child and refuse (at least, most of the time). In a supermarket or a playground, a parent or other observer might see a "stranger" talking to a child. A potential child molester online is not visible. The home used to be a safe haven from pornography and violent or hateful materials. Parents could relax when a child was playing in his or her bedroom. With Internet connections and cellphones, that is no longer true.

3.2.3 Child Pornography and Sexting

Child pornography includes pictures or videos of actual minors (children under 18) engaged in sexually explicit conduct.* Laws against creating, possessing, or distributing child pornography predate the Internet. They cover a broad range of images, many of which would not meet the definition of illegally obscene material if the person depicted were an adult.

Production of child pornography is illegal primarily because its production is considered abuse of the actual children, not because of the impact of the content on a viewer. The adults who produce child pornography often coerce or manipulate children into posing or performing. (The mere possession of child pronography does not directly abuse children, but the Supreme Court accepted the ban on possession on the argument that the buyers or users of the images encourage their production.) It is not automatically illegal to make or distribute sexually explicit movies or photos in which an adult actor plays a minor. In other words, the legal basis for child pornography laws is to prevent using, abusing, and exploiting children, not portraying them. Law enforcement agents regularly make arrests for distribution of child pornography by email, chat rooms, social media, and cellphone. They use surveillance, search warrants, sting operations, and undercover investigations to build their cases and make the arrests.

Congress extended the law against child pornography to include "virtual" children, that is, computer-generated images that appear to be minors, as well as other images where real adults appear to be minors. The Supreme Court ruled that this violated the First Amendment. Justice Anthony Kennedy commented that this extension "proscribes the visual depiction of an idea—that of teenagers engaging in sexual activity—that is a fact of modern society and has been a theme in art and literature throughout the ages."[26]

---

* This is a simplification. The laws include more detail and definitions.

However, the Court accepted a later law that provides harsh penalties for certain categories of computer-generated images and cartoon-type images that appear to be a minor.

Sexting means sending sexually suggestive or explicit text or photos, usually by cellphone or social media. The phenomenon we discuss here involves children, particularly teenagers under 18, sending nude or seminude photos of themselves or their boyfriends or girlfriends to each other or to classmates.* This practice is horrifying to parents, who recognize the dangers it poses to their children. One common result of sexting is severe embarrassment and taunting when the pictures become widely distributed. In an extreme case, after an ex-boyfriend redistributed pictures of an 18-year-old girl, she killed herself. Many young people (like many adults) do not think about how quickly something intended for one person or a small group spreads to a large audience, nor how difficult it is to remove something from cyberspace once it is out there. They do not think about the impact for their future personal and career relationships.

Child pornography laws were intended to apply to adults who commit a repugnant abuse of children. But cellphones and sexting led to application of the laws in unanticipated ways. Prosecutors have brought child pornography charges against children for sexting. Possession of child pornography is illegal, so children who have pictures of friends under 18 on their phones that prosecutors think meet the definition of child pornography are potentially in violation. Is sending nude or sexually suggestive photos of oneself a form of expression? Is it foolish and potentially damaging behavior by an immature person that parents and school officials should deal with? Should it be a criminal felony with severe penalties that can include being put in a sex-offender database for many years?

Some prosecutors may see the threat of prosecution as the only tool they have to stop young people from doing something they will strongly regret in the future. Some may be imposing their moral standards on other people's children. In one case, a 14-year-old girl was prosecuted after refusing a deal that required she attend a counseling class and write an essay about her actions. A court ruled that using a threat of prosecution in this way was to compel speech (the essay) and, thus, violated the First Amendment. Tools that might be useful in schools trying to discourage sexting (such as counseling and essays) are not acceptable when forced by the government.

Legislatures in a few states have revised their state's laws in a variety of ways to reduce the penalties for sexting. Details vary. For example, some have made it a misdemeanor, rather than a felony, if a young person sends an illegal photo to another young person of similar age. Some have reduced or eliminated penalties if photos are distributed (among minors) with the consent of the person in the picture. Revising child pornography laws to deal appropriately with sexting is essential, but that alone is not sufficient. Sexting, and especially distributing explicit photos of schoolmates with the intent to embarrass them,

* Sexting is certainly not limited to teenagers. At least two members of Congress have resigned over sexting scandals.

are problems that should be addressed through education about the consequences of such actions, parental involvement, school policies, reasonable punishments, and so forth.

3.2.4 Spam

What's the problem?

The term *spam*, in the context of electronic communications, was adopted in the 1990s to mean unsolicited bulk email.* It now applies to text messages, tweets, and phone calls as well. Details of a precise definition, depending on how one defines "bulk" and "unsolicited," can be critical to discussions about how to deal with spam, especially when we consider laws to restrict it.

Spam has infuriated users of the Internet since the 1990s. Most, but not all, spam is commercial advertising. Spam developed because email is extremely cheap compared to printed direct-mail advertising. Some businesses and organizations compile or buy huge lists of email addresses and send their unsolicited messages. Some build lists by using automated software that surfs the Web and collects anything that looks like an email address.

Spam angers people because of both the content and the way it is sent. Content can be ordinary commercial advertising, political advertising, solicitations for funds from nonprofit organizations, pornography and advertisements for it, fraudulent "get rich quick" scams, and scams selling fake or nonexistent products. Topics come in waves, with ads for Viagra, ads for low mortgage rates, promotions for various stocks, and Nigerian refugees who need help getting $30,000,000 out of Africa. Some spammers disguise their return address so that bounced mail from closed or invalid accounts does not bother them. ISPs filter out email from known spammers, so many disguise the source and use other schemes to avoid filters. Criminal spammers hijack large numbers of computers by spreading viruses that allow the spammer to send huge amounts of spam from the infected machines, called "zombies."

Spamming for identity theft: Section 5.3

How much spam travels through the Internet? The first case that created an antispam furor involved advertising messages sent by a law firm to 6000 bulletin boards or newsgroups in 1994. At that time, any advertising or postings not directly related to the topic of the group raised the ire of Net users. More recently, one man was accused of running a zombie network that sent billions of emails per day. Another spammer was arrested for clogging Facebook with 27 million spam messages.[27]

Why not just ban spam? We will see some reasons in the next few pages.

---

* Spam is the name of a spiced meat product sold in cans by Hormel Foods. The use of the word in the context of email comes from a Monty Python skit in which some characters repeatedly shouted, "Spam, spam, spam," drowning out other conversation.

Cases and free speech issues

In 1996, about half of the email received at AOL was spam, and a lot of it came from an email advertising service called Cyber Promotions. AOL installed filters to block mail from Cyber Promotions. Cyber Promotions obtained an injunction against AOL's use of filters, claiming AOL violated its First Amendment rights. Thus began the battle over the legal status of spam.

Cyber Promotions' case was weak, and the court soon removed the injunction. Why did AOL have the right to block incoming spam? The spam used AOL's computers, imposing a cost on AOL. AOL's property rights allow it to decide what it accepts on its system. AOL is a membership organization; it can implement policies to provide the kind of environment it believes its members want. Finally, AOL is a private company, not a government institution. On the other side, some civil liberties organizations were uneasy about allowing AOL to filter email because AOL decided what email to block from its members. They argued that because AOL is large, it is a lot like the Post Office, and it should not be allowed to block any mail.

Over the next few years, AOL filed several lawsuits and sought injunctions to stop spammers from sending unsolicited bulk mailings to its members. Notice the subtle shift: Cyber Promotions sought an injunction to stop AOL from filtering out its email. AOL sought injunctions to stop spammers from sending email. Filters do not violate a spammer's freedom of speech, but does an order not to send the mail violate freedom of speech? We listed several arguments why a service provider should be free to filter incoming mail. Do any of the arguments support injunctions against the spammers? One does: the argument that the spam uses the recipient company's property (computer system) against its wishes and imposes a cost on the recipient. AOL and other services won multimillion-dollar settlements from Cyber Promotions and other spammers. But how far does, or should, the owner's control extend? A former Intel employee, Ken Hamidi, maintained a website critical of Intel. He sent six emailings to more than 30,000 Intel employees over a period of less than two years. He disguised his return address, making it difficult for Intel to block his email. Intel sought a court order prohibiting him from sending more email to its employees (at work). Note that in this case the spam was not commercial. Intel argued that freedom of speech gave Hamidi the right to operate his own website, but it did not give him the right to intrude in Intel's property and use its equipment to deliver his messages. Intel argued that the email was a form of trespass. The California Supreme Court ruled in favor of Hamidi. The Court said that Hamidi's bulk emailing was not trespass, because it did not damage Intel's computers or cause economic harm to the company. The dissenting judges argued that Intel's property rights over its computers should allow the company to exclude unwanted email.[28]

Amnesty International has long used its network of thousands of volunteers to flood government officials in various countries with mail when a political prisoner is being tortured or is in imminent danger of execution. Suppose an organization sends the same

An issue for designers and users of filters

We saw that filters are not perfect. They block more or less than the material one wants blocked, and often they block both more and less. If the filter is intended to block sexually explicit material from young children, it might be acceptable to err on the side of blocking some inoffensive material to be sure of preventing the undesirable material from getting through. On the other hand, if the filter is for spam, most people would not mind a few spam messages getting through but would be quite unhappy if some of their nonspam email was thrown away.

email to every member of Congress (or to a list of businesses) each time someone visits the site and clicks to send it. Will we have different points of view about whether this is free speech or spam, depending on how sympathetic we are to the specific organization's message?

Reducing the spam problem

Freedom of speech does not require the intended listener, or message recipient, to listen. Businesses and programmers created a variety of filtering products to screen out spam at the recipient's site, by blocking email from specified addresses, by blocking messages with particular words, and by more sophisticated methods. Many people now see very little spam because their mail service provider filters it out.

Many businesses subscribe to services that provide lists of spammers to block. Aggressive antispam services list not only spammers but also ISPs, universities, businesses, and online services that do not take sufficient action to stop members of their community from sending spam. Such action encourages managers to do something—for example, limit the number of outbound messages from one account. How much discretion should an antispam service have in deciding whom to include on its list of spammers? Harris Interactive, which conducts public opinion surveys by email ("Harris polls"), sued the Mail Abuse Prevention System (MAPS) for including Harris on its blacklist. Harris claimed that the people receiving its email signed up to receive it. MAPS claimed Harris did not meet its standards for assuring the recipients' consent. Harris claimed a competing polling company recommended it for the spammer list.[29] Harris claimed inclusion on the list cut it off from about half of its survey participants and harmed its business. This case illustrates the potential for "gaming" the system by competitors and the differences of opinion that can arise about who is a spammer.

It is interesting to review how attitudes about spam filtering have changed. We saw that when AOL began agressively filtering to block spam, some Internet groups compared the filtering to censorship. Even though AOL was not a government entity, it was large and millions of people received their mail at AOL. People worried that the precedent

of a large corporation filtering email for any reason could lead to corporations filtering email because of content they did not like. Now, many advocacy groups and customers of communications services see spam filtering as valuable and essential.

Spam is cheap. Thus, another idea for reducing it is to increase its cost to the sender. Proposals include certified email schemes and schemes in which email senders pay a tiny charge to the recipient for each email message they send. For certified email, the certifier checks out senders who sign up for the service and, for a small charge per message, certifies that their mail is not spam. The certifier makes agreements with ISPs and email service providers that they deliver certified mail to their members, images and links included, without putting the mail through filters. The messages appear in the recipient's mailbox with an indication that they are "certified."

Many groups object to the very idea of charging any fee to send email. For example, Richard Cox of Spamhaus, an international antispam organization, commented that "an e-mail charge will destroy the spirit of the Internet."[30] Critics say charges might reduce use of email by poor people and nonprofit organizations. Critics of certified mail schemes, such as Spamhaus and the Electronic Frontier Foundation, believe they give ISPs incentive not to improve filters, particularly if the service provider gets part of the certification fee. ISPs also would have an incentive to overfilter—that is, to filter out legitimate email so that more senders will need to pay for certification.

Antispam laws

The impact of antispam laws and decisions about their constitutionality can be quite significant. A man convicted for spamming in Virginia was sentenced to nine years in jail. Virginia's law prohibited anonymous, unsolicited, bulk email. The conviction was reversed when the state's Supreme Court ruled that the law violated the First Amendment. The federal CAN-SPAM Act[31] applies to email sent to computers and mobile devices. It targets commercial spam and covers labeling of advertising messages (for easier filtering), opt-out provisions, and methods of generating emailing lists. Commercial messages must include valid mail header information (that is, faking the "From" line to disguise the sender is prohibited) and a valid return address. Deceptive subject lines are prohibited. Criminal penalties apply for some of the more deceptive practices and for sending spam from someone else's computer without authorization (a process that can be accomplished by viruses that take over another computer).[32] In the first application of the law, four people were charged with sending sales pitches for fraudulent weight-loss products and disguising their identities.

Many antispam organizations opposed the CAN-SPAM Act because they preferred to see spam banned altogether (as it is in some countries), rather than legitimized by the regulation. Many businesses supported CAN-SPAM. The law has been helpful in reducing problem spam from legitimate businesses. We can filter it out and we can get off the mailing list. People who send spam that includes fraudulent "get rich quick" schemes or ads for child pornography clearly do not care about what is legal. They are not likely to

obey laws to identify themselves. Such laws make it easier to fine or jail them by convicting them of violating antispam regulations in cases where there is insufficient evidence for convictions based on the content of the messages.* Is this a benefit or a threat to free speech and due process?

Spammers continually find new ways around spam blockers. The difficulty of distinguishing spam from real mail with absolute certainty suggests that the cycle of new spam techniques and better blocking techniques will continue. Because antispam laws must avoid conflicts with freedom of speech, and because the most abusive spammers ignore laws, laws can reduce spam but are not likely to eliminate the problem.

3.2.5 Challenging Old Regulatory Structures and Special Interests

Most people would not consider ads for wine and real estate on the Web to be offensive material. However, special interest groups tried to remove them. Such groups lobby (often successfully) for laws to restrict uses of new technologies that they see as threats to their income and influence. Most of the cases we discuss here have free speech implications. Several involve regulatory laws that restrict advertising and sales on the Web. Such regulations have noble purposes, such as protecting the public from fraud. They also have the effect of entrenching the already powerful, keeping prices high, and making it more difficult for new and small businesses or independent voices to flourish.

Several companies sell self-help software to assist people in writing wills, premarital agreements, and many other legal documents. The software includes legal forms and instructions for filling them out. It is a typical example of empowering ordinary people and reducing our dependence on expensive experts. A Texas judge banned Quicken legal software from Texas with the argument that the software amounted to practicing law without a Texas license. The Texas legislature later changed its law to exempt software publishers.

When people started publishing online newsletters about certain types of investments, they discovered that they were violating 25-year-old regulations requiring government licenses. License requirements included fees, fingerprinting, a background check, and presenting a list of subscribers on demand to the Commodity Futures Trading Commission (CFTC), the federal agency that administers the regulations. Publishers who did not register with the CFTC could be fined up to $500,000 and jailed up to five years. The regulations were designed for traders who handle other people's money, but the CFTC applied them to people selling investment newsletters or software to analyze commodity futures markets. A federal judge ruled that the CFTC regulations were a prior restraint on speech and violated the First Amendment both for Internet publishers and for traditional newsletter publishers. By raising an issue of free speech on the Web, this case led

* Prohibition-era gangster Al Capone went to jail for income-tax evasion because prosecutors could not convict him of other crimes.

to termination of a long-standing unconstitutional restraint of free speech in traditional media as well.[33]

The Web provides the potential for reducing prices for many products by eliminating the "middleman." Small producers, who cannot afford expensive distributors or wholesalers, can sell directly to consumers nationwide. But not if the business was a small winery. Thirty states in the U.S. had laws restricting the shipping of out-of-state wines directly to consumers. The laws protected large wholesaling businesses that typically get 18%–25% of the price and buy mostly from large wineries or those that sell expensive wines. The laws also protected state revenue; state governments cannot collect sales taxes on many out-of-state sales. State governments argued that the laws prevented sales to minors. This was a weak argument in states that permit direct shipments from in-state wineries. New York also banned *advertising* out-of-state wines directly to consumers in the state. A winery that advertised its wines on the Web ran a risk because the website is accessible to consumers in New York. Winery operators challenged the New York wine law, arguing that it unconstitutionally restricted freedom of speech, interfered with interstate commerce, and discriminated against out-of-state businesses.[34] The Supreme Court ruled that bans on out-of-state shipments directly to consumers were unconstitutional.

The governments of California and New Hampshire attempted to require that operators of websites like ForSaleByOwner.com get state real estate licenses in those states because they list homes for sale within the states. The license requirements are irrelevant and expensive for such sites, and state laws allow newspapers to publish real estate ads, both in the papers themselves and on their websites, without a real estate license. Federal courts ruled that these requirements for real estate licenses violate the First Amendment rights of website operators. The rulings protect the same First Amendment rights for websites as for older media and also reduce the powers of a special interest (in this case, real estate brokers) to restrict competition.

In France, the tax rate on ebooks is 19.6%. The tax on printed books is 5.5%. A law in France prohibits stores from giving big discounts on printed books. Small book sellers asked the French government for similar regulation for ebooks. While I was writing this, the French government planned to reduce the ebook tax but delayed the reduction. Perhaps the popularity of ebooks and discounts will lead to reversal of the old law restricting discounts of printed books.

3.3 Posting, Selling, and Leaking Sensitive Material

> *Free speech is enhanced by civility.*
>
> —Tim O'Reilly[35]

Most of our discussion so far focused on censorship laws, laws prohibiting distribution of or access to certain kinds of material. Legal material that could be sensitive in some way

raises social and ethical issues. Examples include legal "adult" entertainment material, Nazi materials, personal information about other people, and maps and other information that might be of use to terrorists. Intentional publishing of leaked (perhaps stolen) sensitive material for political or social purposes raises social and ethical issues (as well as legal issues). In this section, we consider some of these.

Policies of large companies

Policy reversals by several large websites illustrate some of the dilemmas about posting legal material that is offensive to many people. When Yahoo expanded its online store for adult material (erotica, sex videos, and so forth—all legal), many users complained. Critics objected that because Yahoo is a large, mainstream company, its action gave acceptability to pornography. Yahoo reversed policy and removed ads for adult material. This brought complaints from other people that the company "caved in" to pressure from its mainstream advertisers and users. Some people believe that it is wrong for a large, influential business, like Google, Craigslist, Amazon, or Yahoo, for example, to ban any legal material from its services because the effect is similar to government censorship.

Various online companies have policies against posting hate material, bomb-making information, and other unpleasant or risky material. Apple rejects smartphone apps it finds objectionable; it will not sell them in its app store. Many auctions sites prohibit sales of some kinds of legal products. Large retailers restrict sales to minors of video games with violence, nudity, and sex. Does the legal right of adults to purchase or read something (a negative right, to be free from arrest) impose an ethical or social obligation on a business to provide it? The main justification for an affirmative answer is, as we mentioned above, equating the large social impact of a large company with censorship. On the other hand, in a free society where the government does not decide what we can read or view, it is more important for sellers and individuals to take seriously their role and responsibility in deciding what material they will make available. Also, a private company has property rights in its business that include making decisions about what to sell. If most of the public considers some material inappropriate for mainstream websites and stores, then response to customer pressure will probably keep it from such venues. It will still be available from specialty sites and dealers.

What about search engine providers? Do they have a social or ethical obligation to provide complete search results to all queries, or do they have a social or ethical obligation to omit very offensive sites from search results? The people who set policy in such companies face difficult questions. How should a search engine respond to a search for "nude pictures of college students"? How should it respond to a search for graphic pictures of torture by a government or by terrorists? Search engines provide an extraordinarily valuable and fundamental service. We do not want them to discriminate against unpopular opinions or most forms of controversial material. We want to find news and, sometimes, unpleasant facts. Yet recognition of antisocial or risky uses of some material might lead to ethical decisions to decline to present it prominently, or at all.

A website with risks

Consider websites an individual or small organization might set up. To make the discussion concrete, we consider a site about suicide for terminally ill patients in constant, severe pain. The points we raise here apply to other kinds of sensitive information as well. What should the site organizers consider?* First, even if the site is not advertised, search engines will find it. Depressed teenagers and depressed adults will find it. What we put on a public website is public, available to everyone worldwide. The organizers should think about potential risks and research them. Then what? One option is to decide not to set up the site at all. Suppose the site organizers decide to proceed because they believe their plan has significant value for the intended audience. What can they do to reduce risks? Perhaps require a password to access the site. How would someone obtain a password? Would a simple waiting period reduce the risk for temporarily depressed people? Would the password requirement discourage access by intended users because of privacy concerns? Do you have an ethical responsibility to avoid helping 15-year-olds commit suicide? Can you assume they would find the information to do so somewhere else and that the responsibility to decide is theirs? Do you have an ethical responsibility to help a terminally ill person in pain to commit suicide? Or will your site offer a service some people want but with risks to others that you need to minimize?

People who post risky material have an ethical responsibility to seriously consider questions such as these. The answers are sometimes not obvious or easy. Freedom of speech is not the deciding factor.

Whether thinking about setting up a website with sensitive information or thinking about passing along a funny but embarrassing video of a friend, we sum up a few guidelines: Consider potential risks. Consider unintended readers or users. Consider ways to prevent access by unintended users. Remember that it can be difficult to withdraw material once released.

Leaks

The Web is a convenient and powerful tool for whistleblowers. People can anonymously post documents and make them available to the world. Small organizations and large news companies set up websites specifically to receive and publish leaked documents. Corruption and abuse of power in businesses and governments are common topics. Some leaks serve valuable social purposes. On the other hand, because it is easy to leak a large cache of someone else's documents, people sometimes do so carelessly. Sensitive material, leaked irresponsibly, can harm innocent people.

Throughout, we should remember that leaking begins with a strong ethical case against it. Leaked documents are often obtained by hacking into someone else's computer or by an insider who violates a confidentiality agreement. The documents belong to

* Some people consider suicide itself, and any encouragement of it, to be immoral. For the sake of this discussion, we assume the people setting up the site do not.

someone; they are being stolen or used without the owner's permission. A leak can cause serious damage to a person or organization without their doing anything wrong. Freedom of speech and press do not legitimate stealing files and publishing them, nor do they excuse acting irresponsibly. This does not mean that leaking is always wrong. It means that the reasons for leaking the material must be strong enough to overcome the ethical arguments against it, and the publisher of the leaked material must handle it responsibly.

To analyze the ethics of specific leaks, we consider the type of material released, the value to society, and the risks to society and innocent individuals. We also look at additional issues related to release of very large numbers of documents and some responsibilities of anyone setting up a site to accept and publish leaked material.

Documents that include significant evidence of serious wrongdoing are reasonable candidates for leaks. Wrongdoing might be corruption; political repression; mass murder by armies in international (or internal) wars; serious violations of laws or professional ethics; safety lapses in large systems that affect the public; dishonest practices by a business, scientists, or police; and coverups of such activities—to cite just a very few categories. Another class of documents describe internal discussions and decision making in businesses, organizations, or governments, and candid reports on products and events. There is justification for leaking these if they provide evidence of wrongdoing or risk, but not merely to embarrass people or damage a competitor or organization one disapproves of.

In this discussion, we use two controversial examples that are too broad and complex to fully analyze here. They help to illustrate the questions to consider when evaluating leaks, and—I hope—they generate more discussion. One is the large set of U.S. military and diplomatic documents that WikiLeaks made public.* The other, sometimes called "Climategate," is a collection of emails and other documents from the Climate Research Unit at the University of East Anglia in England, one of the major centers of research on global warming.

The Climategate emails leaked in 2009 and 2011 showed that researchers at the University of East Anglia pursued a variety of methods to deny access to their temperature data by scientists who question some aspects of global warming. Denying access to the data is a violation of scientific practice. The emails also described efforts to stop scientific journals from publishing papers by scientists who are considered skeptics about global warming and to attack the reputations of some of those scientists. Investigations by the British government and other groups concluded that the emails did not show scientific misconduct, but the research center had broken Britain's Freedom of Information Act. The reports criticized various procedures the research group used but not its scientific conclusions. Some emails discussed criticisms and uncertainties related to details of the argument that human activity causes global warming. Researchers discuss such uncertain-

* Earlier, a lot of the material WikiLeaks made public fit reasonable criteria for justifiable, or admirable, leaks. Examples include documents exposing corruption in various governments and exposing murders by police in Kenya.

ties in papers and conferences, but news reports often exclude them. Is it important for the public to know what is in the emails? What criteria argue for or against these leaks?[36]

WikiLeaks released U.S. military documents related to the wars in Iraq and Afghanistan, including videos of shooting incidents. When a long, costly war is controversial, does the public have a right to see the internal reports and vivid video that can inform the debate? Wikileaks released a large set of confidential U.S. diplomatic cables that included, among much else, discussions of the personalities of foreign leaders. Does the value of informing the public outweigh the value of confidential, frank internal discussion when developing diplomatic policies?

When evaluating the ethics of leaking documents on political or highly politicized issues, it can be difficult to make judgments that are independent of our views on the issues themselves. Some people believe that our judgments of the leaks should *not* be independent of the issues: If we oppose U.S. foreign policy, the WikiLeaks leaks are good. If we are skeptical about global warming, the climate research leaks are good. Of course, if we hold the opposite views, we might evaluate the leaks oppositely. This does not help us to develop good criteria for evaluating the ethics of leaking and for guiding us if we come to have access to sensitive data. We can make a much stronger case for ethical criteria by which to evaluate leaks if we are willing to apply the same criteria to leaking similar material on both sides of a political issue.

Potentially dangerous leaks

WikiLeaks released a secret U.S. government cable listing critical sites, such as telecommunications hubs, dams, pipelines, supplies of critical minerals, manufacturing complexes, and so on, where damage or disruption would cause significant harm. Some might defend publication of the list by arguing that it encourages better protection of the sites or that terrorists already know about the sites, but the risks seem to overwhelm any public value of this leak. Other documents detailed discussions between U.S. government officials and an oppostion leader in a country with a very repressive government. Some cables named whistleblowers, confidential informants, human rights activists, intelligence officers, and Chinese people (in business, academia, and the Chinese government) who provided information about social and political conditions in China. The release of these documents put those people at risk. Other documents named people who escaped from repressive countries, potentially endangering their families.* Some leaks do not endanger lives, but they infringe privacy or threaten people's jobs, reputations, freedom, and other values. Those who provide the material and those who publish it have an ethical responsibility to avoid or minimize harming innocent people.[37]

* There were indications that names were removed in some cases. The leaker of the Climategate emails used automated software to remove personal contact information and other personal information in the emails (though some remained, according to some reports).

Releasing a huge mass of documents

The U.S. government documents that WikiLeaks made public included approximately 250,000 diplomatic cables* and thousands of other documents. The Climategate leaks included thousands of documents. Did the leakers review and evaluate all the documents they released to be sure they met reasonable criteria to justify the leaks? Should they have? In the spirit of the Web, leakers can now let the public search through the documents for those of special interest. This can be valuable, but it can be wrong. Recall that an important justification for leaking documents that belong to someone else is that the leaker knows they contain information that the public should see. If the vast majority of the information does not meet the criteria for ethical leaking, then it may be hard to justify publishing the entire set of documents. The documents might be interesting to the public, but in most cases that is not sufficient justification. On the other hand, selective disclosure can distort information by presenting it without context. The best choice might not be easy.

Privacy and confidentiality are important to individuals and to the legitimate functioning of businesses and governments. Privacy and confidentiality are not absolute rights, but they are significant values. Leakers have as much ethical reponsibility to respect privacy (even for people they dislike or disagree with) as do governments and businesses. Thus, justification for overriding privacy and publishing confidential documents should be strong and reasonably specific.

Leaking of government documents is a special case. In some ways it is more justifiable to leak or publish government documents; in other ways less justifiable. The public has a reasonable claim to a right to know what is being done in its name and with its money. On the other hand, criminal investigations and national security often require secrecy. Many states and free countries have laws requiring disclosure of certain public records and laws such as the Freedom of Information Act that allow public access to government records in many situations. The legal processes can be tedious and ineffective sometimes, but the processes should be tried, if they apply, before resorting to hacking to get files or obtaining them from an insider. Sometimes, leaks may be the only way to expose corruption and coverups.

Responsibilities of operators of websites for leaks

Suppose a person or organization decides to establish a site to publish leaked documents that serve an important public purpose. In addition to giving serious consideration to the various points we have raised, the site operators have responsibilities to avoid abuse of the site. The site must have sufficient security to protect the whistleblowers—the people who supply the documents. The operators should have a well-thought-out policy about how to handle requests or demands from law enforcement agencies (of various countries) for

* After Wikileaks released selected cables, the entire set was made public on the Web, either accidentally or intentionally. Either way, failure to protect the documents was a failure of responsibility.

the identity of a person supplying documents. The intent of some leaks is to sabotage a competitor or a political opponent. Verification of the authenticity and validity of leaked documents can be difficult, but it is a responsibility of the site operators. Serious harm to innocent individuals, businesses, economies, and communities can result from publishing inaccurate or forged documents and sometimes from authentic but maliciously leaked documents.

As a German newspaper observed, "When delicate information is at stake, great prudence is demanded so that the information doesn't fall into the wrong hands and so that people are not hurt."[38] Freedom of speech and of the press leave us with the ethical responsibility for what we say and publish.

3.4 Anonymity

> *The Colonial press was characterized by irregular appearance, pseudonymous invective, and a boisterous lack of respect for any form of government.*
>
> —"Science, Technology, and the First Amendment," U.S. Office of Technology Assessment

Common Sense

From the description quoted above, the Colonial press—the press the authors of the First Amendment to the U.S. Constitution found it so important to protect—had a lot in common with the Internet, including controversy about anonymity.

Jonathan Swift published his political satire *Gulliver's Travels* anonymously. Thomas Paine's name did not appear on the first printings of *Common Sense*, the book that roused support for the American Revolution. The Federalist Papers, published in newspapers in 1787 and 1788, argued for adoption of the new U.S. Constitution. The authors, Alexander Hamilton, James Madison, and John Jay, had already served the newly free confederation of states in important roles. Jay later became chief justice of the Supreme Court, Hamilton the first secretary of the Treasury, and Madison president. But when they wrote the Federalist Papers, they used a pseudonym, Publius. Opponents of the Constitution, those who believed it gave too much power to the federal government, used pseudonyms as well. In the 19th century, when it was not considered proper for women to write books, writers such as Mary Ann Evans and Amantine Lucile Aurore Dupin published under male pseudonyms, or pen names (George Eliot and George Sand). Prominent professional and academic people use pseudonyms to publish murder mysteries, science fiction, or other nonscholarly work, and some writers—for example, the iconoclastic H. L. Mencken—used pseudonyms for the fun of it.

Positive uses of anonymity

> *Anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent. Anonymity is a shield from the tyranny of the majority.*
>
> —U.S. Supreme Court

In the United States, the First Amendment protects political speech, but there are still many ways in which the government can retaliate against its critics. There are also many personal reasons why someone might not want to be known to hold certain views. Anonymity provides protection against retaliation and embarrassment. On the Internet, people talk about personal topics such as health, gambling habits, problems with teenage children, religion, and so on. Many people use pseudonyms ("handles," aliases, or screen names) to keep their real identity private. Victims of rape and of other kinds of violence and abuse and users of illegal drugs who are trying to quit are among those who benefit from a forum where they can talk candidly without giving away their identity. (Traditional in-person support and counseling groups use only first names, to protect privacy.) Whistleblowers, reporting on unethical or illegal activities where they work, may choose to release information anonymously. In wartime and in countries with oppressive governments, anonymity can be a life-or-death issue.

Businesses provide a variety of sophisticated tools and services that enable us to send email and surf the Web anonymously. Reporters, human rights activists, and ordinary people use anonymous email to protect themselves. The founder of a company that provided anonymous Web surfing services said the company developed tools to help people in Iran, China, and Saudi Arabia get around their governments' restrictions on Internet access.[40] Many people use anonymous Web browsers to thwart the efforts of businesses to collect information about their Web activity and build dossiers for marketing purposes.

We might think the main benefit of anonymizing services is protection for individuals —protecting privacy, protecting against identity theft and consumer profiling, and protecting against oppressive governments. However, businesses, law enforcement agencies, and government intelligence services are also major customers. A business might want to keep its research and planning about new products secret from competitors. If competitors can get logs of websites that a company's employees visit, they might be able to figure out what the company is planning. Anonymous Web surfing aids law enforcement investigations. Suppose law enforcement agents suspect a site contains child pornography, terrorist information, copyright-infringing material, or anything else relevant to an investigation. If they visit the site from their department computers, they might be blocked or see a bland page with nothing illegal.* Also, when law enforcement agents go "under-

* Websites can determine the IP addresses (that is, the sequence of numbers that identifies a particular domain or computer on the Web) of a visitor and can block access from specified addresses or put up alternate pages for those visitors.

Anonymous remailer services

Johan Helsingius set up the first well-known anonymous email service in Finland in 1993. (Users were not entirely anonymous; the system retained identifying information.) Helsingius originally intended his service for users in the Scandinavian countries. However, the service was extremely popular and grew to an estimated 500,000 users worldwide. Helsingius became a hero to dissidents in totalitarian countries and to free speech and privacy supporters everywhere. He closed his service in 1996 after the Church of Scientology and the government of Singapore took action to obtain the names of people using it. By then, many other similar services had become available.

To send anonymous email using a "remailer" service, one sends the message to the remailer, where the return address is stripped off and the message is re-sent to the intended recipient. Messages can be routed through many intermediate destinations to more thoroughly obscure their origins. If someone wants to remain anonymous but receive replies, he or she can use a service where a coded ID number is attached to the message when the remailer sends it. The ID assigned by the remailer is a pseudonym for the sender, which the remailer stores. Replies go to the remailer site, which forwards them to the original person.

Some anonymity services use encryption schemes to prevent even the company that operates them from identifying the user.

cover" and pretend to be a member or potential victim of an online criminal group, they do not want their IP address to expose them. A senior CIA official explained the CIA's use of anonymity services online: "We want to operate anywhere on the Internet in a way that no one knows the CIA is looking at them."[41]

Negative uses of anonymity

We are not exempt from ordinary ethics and laws merely because we use the Internet or sign comments with an alias rather than a real name.

Anonymity in cyberspace protects criminal and antisocial activities. People use it for fraud, harassment, and extortion, to distribute child pornography, to libel or threaten others with impunity, to steal confidential business documents or other proprietary information, and to infringe copyrights. Anonymous postings can spread false rumors that seriously damage a business, manipulate stock, or incite violence. Anonymity makes it difficult to track wrongdoers. Like encryption, anonymity technology poses challenges to law enforcement.

Anonymity can mask illegal surveillance by government agencies—or legal but repressive surveillance in unfree countries. The CIA helped fund an anonymizer start-up company. The company's anonymity service had flaws that made it possible to determine a user's identity. The company had announced that the CIA had thoroughly reviewed the product, leading to speculation that the CIA knew about the flaws and was happy to have a company offering an anonymizing service that the CIA could circumvent.[42]

Is anonymity protected?

For those not using true anonymity services, secrecy of our identity in cyberspace depends both on the privacy policies of service providers and the sites we visit—and on the laws and court decisions about granting subpoenas for disclosure. How well protected are our real identities? How strongly should they be protected?

A business or organization can get a subpoena ordering an ISP to disclose a person's real identity. In many cases, businesses seek names of people who post criticism, protected by the First Amendment, but who might be employees whom the business would fire. Free speech advocates argue that judges should examine the individual case and determine if the evidence is strong enough that the organization requesting the identity is likely to win a lawsuit—and only then issue a subpoena for the person's real name. Some recommend that ISPs be required to notify a member when the ISP receives a subpoena for the member's identity, so the person has an opportunity to fight a subpoena in court. These suggestions can help protect criticism while holding people responsible for illegal speech.

Because of its potential to shield criminal activity or because they consider it incompatible with politeness and netiquette (online etiquette), some services and online communities choose to discourage or prohibit anonymity. On the other hand, websites that host debate on controversial issues or discussion of socially sensitive topics often consider anonymity to be a reasonable way to protect privacy and encourage open, honest discussion. If those responsible for individual services and websites make policy decisions about anonymity, the policies can be flexible and diverse, adapted to specific services and clienteles.

Many legal issues about anonymity are similar to those in the law enforcement controversies we discussed in Chapter 2. Law enforcement agencies have been able to trace many criminal suspects through the Web (including members of the hacking group called Anonymous). Should it be the responsibility of law enforcement to develop tools to find criminals who hide behind anonymity, or should the task be made easier by requiring that we identify ourselves? Does the potential for harm by criminals who use anonymity to hide from law enforcement outweigh the loss of privacy and restraint on freedom of speech for honest people who use anonymity responsibly? Is anonymity an important protection against possible abuse of government power? Should people have the right to use available tools, including anonymizers, to protect their privacy? We can send hardcopy mail without a return address. Should there be more restrictions on anonymity on the Net than in other contexts?

> *An instance of the inexplicable conservatism and arrogance of the Turkish customs authorities was recently evidenced by the prohibition of the importation of typewriters into the country. The reason advanced by the authorities for this step is that typewriting affords no clew to the author, and that therefore in the event of seditious or opprobrious*

pamphlets or writings executed by the typewriter being circulated it would be impossible to obtain any clew by which the operator of the machine could be traced . . . . The same decree also applies to mimeograph and other similar duplicating machines and mediums.

—*Scientific American*, July 6, 1901[43]

3.5 The Global Net: Censorship and Political Freedom

The coffee houses emerged as the primary source of news and rumor. In 1675, Charles II, suspicious as many rulers are of places where the public trades information, shut the coffee houses down.

—Peter L. Bernstein[44]

3.5.1 Tools for Communication, Tools for Oppression

Authoritarian governments have taken steps to cut, or seriously reduce, the flow of information and opinion throughout history.* The vibrant communication made possible by the Internet threatens governments in countries that lack political and cultural freedom. For a long time, the "conventional wisdom" among users and observers of the Internet was that it is a protection against censorship and a tool for increased political freedom. Email and fax machines played a significant role during the collapse of the Soviet Union and the democracy demonstrations in China's Tiananmen Square. Websites with content that is illegal in one country can be set up in some other country. People in countries that censor news can access information over the Web from elsewhere. Facebook and cellphones were key tools in organizing the 2011 Arab Spring. Dissidents in Iran, Vietnam, various Middle Eastern countries, and elsewhere use Skype to communicate because of its strong encryption. There are many more examples.

Unfortunately, but not surprisingly, oppressive governments learned and adopted countermeasures to block the flow of information. They use sophisticated interception and surveillance technologies to spy on their citizens more thoroughly than before. In the rest of this section, we describe censorship and interception tools that oppressive regimes (and some democracies) use.

In countries such as China and Saudi Arabia, where the national government owns the Internet backbone (the communications lines and computers through which people access information), the governments install their own computers between their people and the

* In Poland, for example, before the communist government fell in 1989, it was illegal to make a photocopy without permission from government censors. Other governments have banned satellite dishes and residential telephones.

outside world. They use sophisticated firewalls and filters to block what they do not want their people to see. The government of Saudi Arabia blocks pornography and gambling, as many countries might, but it also blocks sites on the Bahai faith, the Holocaust, and religious conversion of Muslims to other faiths. It blocks sites with information about anonymizers, tools to thwart filters, and encryption.

Turkey banned YouTube for about two years. Pakistan banned Internet telephony. Burma (Myanmar) banned use of the Internet or creation of Web pages without official permission. It banned posting of material about politics, as well as posting of any material deemed by the government to be harmful to its policies. (Under an earlier law, possession of an unauthorized modem or satellite dish was punishable by a jail term of up to 15 years.) Many countries in the Middle East limit Internet access. Vietnam uses filtering software to find and block anticommunist messages coming from other countries.*

Some countries ban Skype. Others subvert it. Before the revolution in Egypt in 2011, the Egyptian government, for example, used spyware to intercept Skype communications. They did not break Skype's encryption scheme. Instead, it appears they planted spyware on people's computers that intercepted a communication before it was encrypted on the sender's computer or after it was decrypted on the recipient's computer. During the revolution, the government temporarily shut down the Internet and cellphone service entirely.

In the 1990s, when fewer people used the Web, the Chinese government required users of the Internet to register with the police. In China and other long-unfree countries, governments are struggling with the difficulties of modernizing their economy and technology while maintaining tight control over information. Now, with hundreds of millions of Web users, the government strictly controls and censors what people read and what they post. Chinese regulations prohibit "producing, retrieving, duplicating and spreading information that may hinder public order." Banned or censored sites and topics have included Facebook, Google, the *New York Times*, discussion of democracy, religious sites, human rights organizations, news and commentary about Taiwan and Tibet, information about censorship (and how to evade it), economic news, and reports of major accidents or natural disasters and outbreaks of diseases. The government blocked both the Chinese-language and English-language Wikipedia sites for about a year. Thousands of censors monitor websites. When Chinese citizens began texting to communicate about banned topics, the government set up a system to filter the messages.[45] After ethnic protests turned violent in one region, China cut communications, then blocked Internet access in the region for 10 months.

The government of Iran, at various times, blocked the sites of amazon.com, Wikipedia, the *New York Times*, and YouTube. It also blocked a site advocating the end of the

* Where the technology has not caught up, governments restrict old communications media. A rival of Zimbabwe's president Robert Mugabe in Zimbabwe's 2001 presidential election was charged with possession of an unlicensed two-way radio.

practice of stoning women. Reporters Without Borders said that Iran blocked access to more than five million websites in recent years. Generally, the government says it blocks sites to keep out decadent Western culture. Iran also jams satellite TV broadcasts. The government uses sophisticated online surveillance tools and trained cyber police to spy on dissidents. Their system examines individual packets of email, phone conversations, images, social-network communications, and so forth.

In some countries, government agents, using social media, pretend to be dissidents and distribute information about planned protests; the police arrest anyone who comes. Some governments (e.g., Tunisia and Libya before the revolutions in 2011) intercepted communications and used spyware on sites such as Facebook and Yahoo to collect passwords, find the names of dissident bloggers, and take down pages critical of the government. Some governments (e.g., China, Iran, Russia, Vietnam) ban or discourage email services and social networking sites based in the West and set up their own—which, of course, they control.[46] As we will see in Section 3.5.2, restrictive governments are increasingly using their leverage over companies that want to do business in their countries to enforce censorship requirements and other content standards.

Will the Internet and related communications technologies be tools for increasing political freedom, or will they give more power to governments to spy on, control, and restrict their people?

> *The office of communications is ordered to find ways to ensure that the use of the Internet becomes impossible. The Ministry for the Promotion of Virtue and Prevention of Vice is obliged to monitor the order and punish violators.*
>
> —Excerpt from the Taliban edict banning all Internet use in Afghanistan, 2001[47]

3.5.2 Aiding Foreign Censors and Repressive Regimes

> *Freedom of expression isn't a minor principle that can be pushed aside when dealing with a dictatorship.*
>
> —Reporters Without Borders[48]

Providing services, obeying local laws

Search engine companies, social media companies, and news and entertainment companies based in free countries offer services in countries with strict censorship and repressive governments. To operate within a country, companies must follow the laws of the country. What are the trade-offs between providing services to the people and complying with the government's censorship requirements? To what extent does, or should, the prospect

of a huge business opportunity in a new country affect a company's decision? How do companies deal with the censorship requirements? What are their ethical responsibilities?

The Chinese sites of Yahoo and MSN comply with local law and omit news stories that offend the government. Microsoft said it censored terms like "freedom" and "democracy" on its Chinese portal. Microsoft also shut down a Chinese journalist's blog on its MSN Spaces site that criticized the Chinese government.[49] Yahoo provided information to the Chinese government that helped identify at least two people who were then jailed for pro-democracy writing. Yahoo said it was required to comply with Chinese law and the company had not been told the reason for the government request for the information.

To operate in China, the Chinese government requires Skype to work in a joint venture with a Chinese communications company (TOM), use a modified version of the Skype software, and filter out sensitive topics from text chat. According to a study by a Canadian university, the modified software allowed widespread surveillance, and TOM stored information from millions of messages.

Google has long promoted the ideal of access to information. Google held out longer than some companies, refusing to censor its search engine, although it had taken some steps toward restricting access to information in China. In 2006, Google disappointed many free speech and human rights advocates by introducing a Chinese version in China, google.cn, that would comply with Chinese law. Its search results did not show sites with banned content. Google concluded that the company could not provide a high level of service in China without a local presence. Thus, the agreement to operate in China and block material the government considers sensitive was a decision that some access is better than no access. Google co-founder Sergey Brin, who was born in the Soviet Union and experienced totalitarian government, was uneasy with the 2006 censoring decision. Google stopped operating the censored search engine in 2010. The company withdrew most operations from China but offered its search service through Hong Kong, which, though part of China, has different laws. The main impetus for the change was a highly sophisticated hack attack originating in China on Google and about 30 other companies. A primary goal of the attack appeared to be access to Gmail accounts of Chinese human rights activists, angering Brin and others at Google. Google's initial refusal to censor, its reversal in 2006, and its reversal again in 2010 illustrate the difficulty of deciding how to deal with repressive governments. Later, Google increased operations in China not subject to censorship, such as product searching and the Android operating system.

When U.S. or other non-Chinese companies set up branches in China and comply with restrictive laws, should we view them as providing more access to information in China than would otherwise exist, albeit not as much as is technically possible? Should we view them as appropriately respecting the culture and laws of the host country? Should we view them as partners in the Chinese government's ethically unacceptable restrictions on debate and access to information by its citizens?

Mark Zuckerberg, CEO of Facebook, suggested that the advantages of social networking in China outweigh the restrictions. We can view this argument, similar to the

arguments from other companies for complying with demands of authoritarian governments, as a utilitarian argument. If a company turns over the names of people who violate censorship laws, the government arrests a small number of dissidents, but a very large number of people benefit from the increased services and communications. If one considers longer-term effects, however, one must consider that the work of a small number of dissidents can have a huge impact on the freedom of the society as a whole. One can make other utilitarian arguments (strong and weak). The arrest of a dissident might spur a protest ultimately bringing more freedom—or a brutal crackdown. A rights-based ethical system might accept providing a search or social media service that is somewhat limited. The people have the right (ethical, even if not legal) to seek and share information, but the service provider is not ethically obligated to provide it 100%. However, a rights-base view tells us it is wrong to help jail a person for expressing his views on politics or for criticizing the government. Should companies draw a line, perhaps agreeing to restrict access to information but refusing to disclose information that a government can use to jail someone for publishing his or her views? A government might need to identify a person whom it suspects of stalking, fraud, posting child pornography, or other crimes. A service provider might want to provide information in such criminal cases. If the government does not disclose the reason for a request, or is dishonest about the reason, how can a service provider make an ethical decision?

> *We're allowing too much, maybe, free speech in countries that haven't experienced it before.*
>
> —Adam Conner, a Facebook lobbyist[50]

> *Don't be evil.*
>
> —Google's informal corporate motto

Selling surveillance tools

It is perhaps not surprising that repressive governments intercept communications and filter Internet content. It is disturbing that companies in Western democracies (including England, Germany, France, and the United States) sell them the tools to do so. Companies sell governments sophisticated tools to filter Internet content, to hack cellphones and computers, to block text messages, to collect and analyze massive amounts of Internet data, to plant spyware and other malware (malicious software), to monitor social networks, and to track cellphone users. The companies say the tools are for criminal investigations (as well as detecting and filtering undesirable content) and do not violate the laws of the country using them. Of course, countries with repressive governments have criminals and terrorists too. Do we trust these governments to use the tools only against the bad guys, in ways consistent with human rights? Is it ethical for companies in free countries to sell the tools to repressive governments?

> *We don't really get into asking, "Is this in the public interest?"*
>
> —An organizer of a trade show for companies selling hacking and interception gear to governments[51]

3.5.3 Shutting Down Communications in Free Countries

Governments in relatively unfree countries that tightly control communications shut down access to the Internet or shut down cellphone service now and then. These events evoke criticism in the free world, where few expected it could happen. Then the British government and some U.S. cities considered it, and the transit system in San Francisco blocked cellphone service for a few hours, raising new issues for communications in free countries. Giving governments authority to shut down communications poses obvious threats to freedom of speech, ordinary activities, and political liberty. Is it reasonable in limited situations when public safety is at risk? Does shutting communication services in free countries give excuses to dictators? Can we make a clear distinction between short-term responses to violent mobs in free countries and censorship and repression of political discussion in unfree countries? As background for thinking about these questions, we consider the incidents in Britain and the United States.

Mobs of hooligans (that old-fashioned word seems to fit) rampaged through neighborhoods in London and other British cities setting fires, looting businesses, and beating up people who tried to protect themselves or their property. They planned and coordinated their attacks using cellphones, Twitter, BlackBerry Messenger, and similar tools. During the violence, people in the government (and others) argued that Research In Motion should shut down BlackBerry Messenger. (It did not.) After the riots, the British government considered seeking legislation authorizing it to shut down communications systems such as social media and messaging systems in such situations. It decided, at least for the time being, not to seek such power. Several U.S. cities that experienced similiar coordinated violence considered laws to authorize government agencies to block communications, but none passed such laws.

Shortly after the violence in England, the Bay Area Rapid Transit system (BART) in the San Francisco Bay Area shut off wireless service in some of its subway stations after learning of a plan to "use mobile devices to coordinate . . . disruptive activities and communicate about the location and number of BART Police."[52] BART owns the communications equipment; it said its contracts with cell service companies allow it to shut off the service when it thinks necessary. The managers of a private business, expecting violence on or near their property, have the right to shut off their wireless service; refuse entry to anyone carrying, say, a baseball bat; or close up if they think it a wise measure to protect the public and the business. If BART were a private company, there would be arguments on both sides of the question of whether its action was wise, but it would not raise the First Amendment issues of a government-ordered shutdown. (Some of the arguments, and the distinction between government and private action, are similar to those concerning the right of a computer service to filter out spam; see Section 3.2.4.)

BART is a government agency, but it shut down its own wireless service in its own space. Did it threaten freedom of speech, or was it a legitimate safety decision?

What can be done, short of shutting down communications, to reduce the use of such systems for planning mass violence? The membership policies of various social media companies ban threats of violence. Facebook, for example, monitors posts to enforce its ban. The companies can close the accounts of those who violate the agreements, but it is unlikely that such companies would be able to act quickly enough to stop a violent event. In past riots, police collected information from social media and phones of people they arrested, and in doing so they learned of plans for more violent attacks and were prepared to prevent them. While helpful, this also seems like weak protection. But what are the consequences of giving governments the authority to shut down communications? Police can abuse this power, preventing legitimate protests and demonstrations, as repressive governments do. A large-scale shut down would inconvenience (and possibly harm) innocent people. In the United States, the Supreme Court would probably declare unconstitutional a law that authorized a government agency to order a private communications service to shut down. What else can be done?

> *It may be BART's equipment, but that doesn't mean that they have the freedom to do whatever they want to with it.*
>
> —Michael Risher, ACLU attorney[53]

3.6 Net Neutrality Regulations or the Market?

Direct censorship is not the only factor that can limit the amount and variety of information available to us on the Internet. The regulatory structure affects the availability of services and the degree of innovation. Large companies often lobby for laws and regulations to restrict competition: The U.S. television networks delayed cable for more than a decade. For decades, broadcasting companies lobbied to keep low-power radio stations (called "micro radio") virtually illegal. "Net neutrality" refers to a variety of proposals for restrictions on how telephone and cable companies interact with their broadband customers (primarily for Internet services) and how they set charges for services. There are two different but related issues, sometimes blurred in the arguments: (1) whether the companies that provide the communications networks should be permitted to exclude or give different treatment to content based on the content itself, on the category of content, or on the company or organization that provides it, and (2) whether the companies that provide the communications networks should be permitted to offer content providers and individual subscribers different levels of speed and priority at different price levels. The latter is sometimes called "tiered" service—that is, different levels of service with different charges. Very large companies are on both sides of the debate, as are organizations and prominent people who want to preserve the openness and vitality of the Net.

Advocates of "net neutrality" want the government to mandate that telecommunications companies treat all legal content that travels through their broadband lines and wireless networks the same way. Equal treatment includes charging all customers the same rate for sending information over the Internet and not giving priority to any particular content or customer. Net neutrality would restore part of the concept of common carrier (as described in Section 3.1), based partly on the view that telephone companies (now telephone and cable) have a monopoly on transmission of information and that companies that control transmission should not be permitted to control access to content as well. Many Internet content providers, including individual bloggers and large companies such as eBay, Microsoft, Amazon, Netflix, and Google, argue for net-neutrality rules. Without the rules, some argue, they will have to pay higher rates and communications companies will give special treatment to their own content providers. Some groups argue that allowing communications companies to set varying rates would be devastating for the Internet as it would squeeze out independent voices.

Charging different rates for products and services is not unusual and makes economic sense in many areas. Research journals charge libraries a higher subscription rate than they charge individuals, because more people read each library copy. Many businesses give large-quantity discounts. Some institutions and businesses—hospitals, for example—pay a higher rate for services such as electricity under contracts that guarantee higher priority for repairs or emergency service when necessary. We all have a choice of paying standard delivery charges for products we buy online or paying more for faster delivery. People pay to drive in express lanes on freeways; the price might vary with the time of day and level of traffic. Thus, the notion that every customer should pay the same amount does not have intrinsic merit. Does it have merit for the Internet? Would it make sense for communications carriers to, say, contract with video suppliers to provide faster delivery of videos for a fee?

Supporters of neutral pricing fear that lack of pricing regulation will erode the diversity of the Internet. Only big companies and organizations will be able to afford the prices necessary to ensure that their content moves fast enough to be relevant. Content that individuals and smaller organizations provide will get lost. Some argue that flexible pricing will give telecommunications companies too much power over content on the Internet. Supporters of net neutrality see tiered service as a threat to innovation, democratic participation, and free speech online. Vinton Cerf, Vice President and Chief Internet Evangelist at Google* and a highly respected Internet pioneer, sees the neutrality of the carriers, the lack of gatekeepers and centralized control, as key factors responsible for the success of the Net and innovations like blogging and Internet telephony. He argues that there is not enough competition in the network operator industry to protect against abuses.[54]

* Really, that's his title.

Opponents of net neutrality argue that neutrality regulations will slow the advance of high-speed Internet connection and improvements in infrastructure. Before the FCC relaxed older regulations (in 2003–2005), telecommunications companies had little incentive to invest in broadband capacity. In the few years afterward, they invested hundreds of billions of dollars. Speeds increased, prices fell, and the added capacity was essential for new phenomena such as streaming movies. Continued investment in broadband is necessary for growth in areas such as online backup services, all the data we receive on cellphones, applications of remote sensors, innovations in education services, and so on. Opponents of additional regulations say there should be no major new regulation without evidence of harm in the current system. David Farber, another highly respected Internet pioneer, opposes neutrality legislation: "We don't want to inadvertently stall innovation by imposing rules or laws the implications of which are far from clear."[55] Some who support free markets oppose mandated uniform pricing on principle, as an unethical interference in the free choices of sellers and buyers.

The huge surge in traffic due to smartphones and tablets heightened issues of net neutrality. By 2010, video made up more than 75% of mobile data traffic. Does it make sense to treat such traffic differently? Should it have high priority (like voice calls) because delays are annoying to the customer? Should it have lower priority because it uses so much bandwidth? Should service providers make these decisions, or should Congress and the FCC make them? When people watch a video on a smartphone, they often do not watch the whole thing. A company developed techniques to send a video to the user in segments as he or she watches (without increasing delays), rather than sending the entire video as fast as possible. The company said this approach could cut data transfer in half. Can regulators write net neutrality rules that allow or encourage such technological solutions for reducing traffic, or will rigid rules stifle or discourage them?

The legal status of net neutrality is still unclear. When Comcast slowed some traffic from certain specific sites in 2007, the FCC said the company violated FCC guidelines and ordered it to stop. A federal court ruled that the FCC did not have legal authority to do so. Congress has not given the FCC authority to make rules for the Internet. The FCC issued rules, anyway, in 2011; court challenges are underway.

EXERCISES

Review Exercises

3.1 Briefly explain the differences between common carriers, broadcasters, and publishers with respect to freedom of speech and control of content.

3.2 Describe two methods parents can use to restrict access by their children to inappropriate material on the Web.

3.3 What was one of the main reasons why courts ruled the censorship provisions of the Communications Decency Act in violation of the First Amendment?

3.4 What is one way of reducing spam?

3.5 What documents did WikiLeaks make public?

3.6 Give an example of an anonymous publication more than 100 years ago.

3.7 Mention two methods some governments use to control access to information.

General Exercises

3.8 A large company has a policy prohibiting employees from blogging about company products. What are some possible reasons for the policy? Does it violate the First Amendment? Is it reasonable?

3.9 How has the Internet changed the notion of community standards for determining if material is legally obscene? Do you think the community standards criterion can be preserved on the Internet? If so, explain how. If not, explain why.

3.10 What policy for Internet access and use of filter software do you think is appropriate for elementary schools? For high schools? Give your reasons.

3.11 Various organizations and members of Congress suggest requiring Web sites that contain material "harmful to minors" to move to a new Web domain ".xxx". Give some reasons for and against such a requirement.

3.12 A bill was introduced in Congress to require that websites with pornography get proof of age from anyone who tries to visit the site, possibly by requiring a credit card number or some other adult identification number. Discuss some arguments for and against such a law.

3.13 Library staff members in two cities filed complaints with the federal Equal Employment Opportunity Commission (EEOC) arguing that they were subjected to a "hostile work environment." The libraries where they worked did not provide filters on Internet terminals. Staffers were forced to view offensive material on the screens of library users and pornographic printouts left on library printers. Discuss the conflict between a hostile work environment and freedom of speech in this situation. Without considering the current laws, how would you resolve the conflict here?

3.14 Four high school students found instructions for making a bomb on a website. They built the bomb and set it off in the hallway of their school. One of the students, an 18-year-old, said they had no idea how powerful the bomb would be and they had no intention of hurting anyone. He commented, "These are really dangerous sites. . . . I'm not a troublemaker or anything. I'm just a regular kid."[56] Evaluate his comments.

3.15 Suppose you are writing an antispam law. What do you think is a reasonable definition of spam in this context? Indicate the number of messages and how the law would determine whether a message was unsolicited.

3.16 Federal regulations and laws in some states (some long-standing, some passed specifically for the Internet) prohibit or restrict many kinds of online sales. For example, laws restrict sale of contact lenses, caskets, and prescription medicines on the Web. Laws prohibit auto manufacturers from selling cars directly to consumers on the Internet.* The Progressive Policy Institute estimated that such state laws cost consumers at least $15 billion a year.[57]

For which of these laws can you think of good reasons? Which seem more like the anticompetitive laws described in Section 3.2.5?

---

* The specific items whose sale or purchase online is prohibited or restricted may have changed.

3.17 In Section 3.3, we saw that people criticized Yahoo for expanding its online store for adult material, and people criticized Yahoo for responding to complaints, reversing the new policy, and removing ads for adult material. What do you think of Yahoo's decisions? What do you think of both criticisms?

3.18 A website that publishes leaked documents posts the contents of the Yahoo email account of a candidate for president during the election campaign.

(a) Describe some types of things that might be among the leaked documents that would be valuable to opponents of the candidate.

(b) Describe some things that might be among the leaked documents that could hurt a campaign but do not indicate any wrongdoing.

(c) Devise standards for the ethics of posting the contents of the account that you would be comfortable with no matter whether you support or oppose the candidate.

3.19 You are aware of a study that concludes that California's emergency systems, including hospitals, emergency supplies, police, and so forth, are not sufficient for responding to the magnitude of earthquake likely to occur in the next 30 years. The study has not been released to the public, and you are thinking of leaking it to a website that publishes leaked documents. List benefits of leaking the study and risks of doing so. List any other questions you consider relevant to making the decision. Indicate how different answers to some of the questions might affect your decision.

3.20 Amateur astronomers around the world have been locating and tracking satellites—both commercial and spy satellites—and posting their orbits on the Web.[58] Some intelligence officials argue that if enemies and terrorists know when U.S. spy satellites are overhead, they can hide their activities. What issues does this problem raise? Should astronomers refrain from posting satellite orbits? Why, or why not?

3.21 Someone posted a video on a popular video site showing a group of men with clubs enter a building and beat unarmed people. The site's policy prohibits posting videos with graphic violence. When a viewer complained, the site removed the video. Other viewers appealed the removal, saying the video documented abuse of prisoners in a Russian prison camp. Suppose you are a manager at the site. Develop a plan for dealing with such videos. Will you repost the video? Explain the issues you considered.

3.22 An antiabortion website posted lists of doctors who perform abortions and judges and politicians who support abortion rights. It included addresses and other personal information about some of the people. When doctors on the list were injured or murdered, the site reported the results. A suit to shut the site for inciting violence failed. A controversial appeals court decision found it to be a legal exercise of freedom of speech. The essential issue is the fine line between threats and protected speech, a difficult issue that predates the Internet. Does the fact that this is a website rather than a printed and mailed newsletter make a difference? What, if any, issues in this case relate to the impact of the Internet?

3.23 The European Union has laws that restrict the percentage of audio-visual media programming (originally primarily television, but now including Internet content) produced outside the EU. Canada has similar restrictions on radio and television content. People in the Canadian film industry have proposed quotas on foreign movies. The reasons given include protecting a country's culture and protecting their content companies from foreign competition.

(a) Do you think such restrictions are reasonable? Do you think they will remain effective with the expansion of online media in recent years? Give reasons.

(b) The United States does not have such quotas on foreign programming or movies. Why do you think this is the case?

3.24 It is illegal for tax-exempt charitable groups to do political lobbying. The websites of many such organizations have links to sites of organizations that do lobbying. For example, a tax-exempt think tank has links to Handgun Control, Inc. and the National Rifle Association, so visitors can find relevant research materials on both sides of gun-control issues. The Internal Revenue Service (IRS) announced an investigation into whether such links violate the rules for tax-exempt status. What do you think they should conclude? How would various possible decisions by the IRS affect the Web?

3.25 A company sells spyware that can intercept and record phone communications and email on a variety of email services. The company sells the software to government agencies in the United States (or your country, if you are outside the United States) that want it to pursue criminals and terrorists. Using ethical criteria from Chapter 1 and legal or constitutional criteria (from Chapter 2 as well as this one, or based on your country's constitution if you are outside the United States), evaluate the decision to sell the software.

3.26 Using ethical criteria from Chapter 1, evaluate the decision to sell the software described in the previous exercise to a repressive government.

3.27 In Section 3.6, we discussed arguments about proposals for charges for faster delivery of content over the Internet. What do you think are likely impacts of such charges? Give reasons. Use analogies from other fields.

3.28 Assume you are a professional working in your chosen field. Describe specific things you can do to reduce the impact of any two problems we discussed in this chapter. (If you cannot think of anything related to your professional field, choose another field that might interest you.)

3.29 Think ahead to the next few years and describe a new problem, related to issues in this chapter, likely to develop from digital technology or devices.

Assignments

These exercises require some research or activity.

3.30 Find out whether your college restricts access to any websites from its computer systems. What is its policy for determining which sites to restrict? What do you think of the policy?

3.31 At the time I wrote this, Facebook, banned in China since 2009, planned to establish a presence there. It would have to comply with China's censorship requirements and requirements to provide user information to the government. Is Facebook now in China? If so, how has it dealt with the censorship and reporting requirements?

Class Discussion Exercises

These exercises are for class discussion, perhaps with short presentations prepared in advance by small groups of students.

3.32 Under laws in Germany that protect the privacy of criminals who have served their sentence, a murderer took legal action to force Wikipedia to remove its article about his case. Discuss the conflict between privacy and freedom of speech raised by this case.

3.33 To what extent is violent material on the Web and in computer games responsible for shootings in schools? What should be done about it, without violating the First Amendment?

3.34 A computer system manager at a public university noticed that the number of Web accesses to the system jumped dramatically. Most of the increased accesses were to one student's home page. The system manager discovered that his home page contained several sexually oriented pictures. The pictures were similar to those published in many magazines available legally. The system manager told the student to remove the pictures. A female student who accessed the pictures before they were removed filed a grievance against the university for sexual harassment. The student who set up the home page filed a grievance against the university for violation of his First Amendment rights.

Divide the class into four groups: representatives for the female student, the male student, and the university (one group for each grievance). A spokesperson for each group presents arguments. After open discussion of the arguments, take a vote of the class on each grievance.

3.35 The CAN-SPAM law applies to commercial email; political messages are exempt. Present arguments that laws to restrict or regulate spam should treat both categories of bulk email the same way. Present arguments to justify different treatment of these two categories.

3.36 Discuss the questions in Section 3.3 about ethical responsibilities for setting up a website with information about suicide for terminally ill people in pain. Discuss analagous questions for setting up a website with information about how to make explosives for a legitimate purpose (perhaps demolition or clearing farm land). If answers differ for the two situations, identify the attributes or principles that lead to different answers.

3.37 After an incident of nasty verbal attacks and death threats to a blogger from people who disagreed with something she wrote, Tim O'Reilly and Jimmy Wales proposed a Bloggers Code of Conduct. Find a copy of the code that developed from this proposal (or another code of conduct for bloggers). Evaluate it. Discuss its compatibility with freedom of speech. Should bloggers follow the code?

3.38 Is the control that large companies such as Google have over Internet search results a threat to freedom of speech?

3.39 Should Skype continue to operate in China under the joint venture with TOM, as described in Section 3.5.2? Why or why not?

3.40 (a) In a riot such as the one in England in 2011, where rioters planned and coordinated their activites using (among other things) BlackBerry Messenger, should Research In Motion (RIM) shut down Messenger temporarily? Assume the government does not have the legal authority to order the shut down, but law enforcement agencies and government officials have asked RIM to shut the service to prevent more violence.

(b) A cybersecurity bill in the U.S. Senate (which did not pass) had a provision that some critics believed could have given the government authority to shut down the Internet in an emergency. Should the government have such authority?

3.41 The net neutrality rules issued by the FCC in 2011 treated wired and wireless communication networks differently (allowing more flexibility to operators of wireless networks). Give some reasons for treating them differently. Give some reasons why they should be treated the same. What do you think makes the most sense?

BOOKS AND ARTICLES

- Floyd Abrams, *Speaking Freely: Trials of the First Amendment*, Viking Penguin, 2005.
- Robert Corn-Revere, "Caught in the Seamless Web: Does the Internet's Global Reach Justify Less Freedom of Speech?" Cato Institute, July 24, 2002.
- Electronic Privacy Information Center, *Filters and Freedom 2.0: Free Speech Perspectives on Internet Content Controls*, www.epic.org, 2001.
- Mike Godwin, *Cyber Rights: Defending Free Speech in the Digital Age*, Times Books, Random House, 1998.
- Marjorie Heins, *Not in Front of the Children: "Indecency," Censorship, and the Innocence of Youth*, Hill & Wang, 2001.
- Nat Hentoff, *Free Speech for Me—But Not for Thee: How the American Left and Right Relentlessly Censor Each Other*, Harper Collins, 1992.
- Peter Huber, *Law and Disorder in Cyberspace*, Oxford Univ. Press, 1997. Criticizes FCC regulation of telecommunications, showing examples where regulations have delayed introduction of new technologies.
- Anthony Lewis, *Freedom for the Thought That We Hate: A Biography of the First Amendment*, Basic Books, 2008.
- Lyrissa Barnett Lidsky, "Silencing John Doe: Defamation and Disclosure in Cyberspace," *Duke Law Journal*, 49:4, February 2000, pp. 855–946. (Available at www.law.duke.edu.)
- Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom*, Basic, 2012.
- Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom*, PublicAffairs, 2011.
- "Science, Technology, and the First Amendment, Special Report," Office of Technology Assessment, U.S. Dept. of Commerce, Washington, DC, Jan. 1988 (Report NO. OTA-CIT-369).
- Scott Shane, *Dismantling Utopia: How Information Ended the Soviet Union*, I. R. Dee, 1994.
- Ithiel de Sola Pool, *Technologies of Freedom*, Harvard University Press, 1983. This book describes the history, rights, restrictions, and responsibilities of the various communications technologies in depth.
- Eugene Volokh, "Freedom of Speech in Cyberspace from the Listener's Perspective: Private Speech Restrictions, Libel, State Action, Harassment, and Sex," *Univ. of Chicago Legal Forum*, 1996, pp. 377–436.
- Tim Wu, *The Master Switch: The Rise and Fall of Information Empires*, Knopf, 2010.

NOTES

1. From a speech by Mike Godwin at Carnegie Mellon University, November 1994, quoted with permission. (The speech is excerpted, including part of the quotation used here, in Mike Godwin, "alt.sex.academic.freedom," *Wired*, February 1995, p. 72.)
2. "Internet 2010 in Numbers," Pingdom, royal.pingdom.com/2011/01/12/internet-2010-in-numbers, viewed Nov. 22, 2011.
3. Eric M. Freedman, "Pondering Pixelized Pixies," *Communications of the ACM*, August 2001, 44:8, pp. 27–29.
4. "High Court Rules Cable Industry Rights Greater Than Broadcast's," *Investors Business Daily*, June 28, 1994.
5. Title V, Section 230.
6. Advertising wine on the Internet was protected in a 2006 case in Minnesota. Earlier cases concerned advertising of

tobacco, legal gambling, vitamin supplements, alcohol content of beer, prices of prescription drugs, and Nike's claim that it did not use sweatshop labor. Lee McGrath, "Sweet Nector of Victory," *Liberty & Law*, Institute for Justice, June 2006, vol. 15, no. 3, pp. 1, 10. Robert S. Greenberger, "More Courts Are Granting Advertisements First Amendment Protection," *Wall Street Journal*, July 3, 2001, pp. B1, B3.

7. In *The Life of Voltaire*, Smith, Elder & Company, 1904. See also Fred S. Shapiro, ed., *The Yale Book of Quotations*, Yale University Press, 2007. The quotation is often incorrectly attributed to Voltaire himself.
8. Gerard van der Leun, "This Is a Naked Lady," *Wired*, Premiere Issue, 1993, pp. 74, 109.
9. Dick Thornburgh and Herbert S. Lin, eds., *Youth, Pornography and the Internet*, National Academy Press, 2002, books.nap.edu/catalog/10261.html.
10. Mike Godwin, "Sex, Cyberspace, and the First Amendment," *Cato Policy Report*, Jan./Feb. 1995, 17(1), p. 10.
11. Robert Peck, quoted in Daniel Pearl, "Government Tackles a Surge of Smut on the Internet," *Wall Street Journal*, Feb. 8, 1995, p. B1.
12. For a commentary on the many issues in this case, see Mike Godwin, "Virtual Community Standards," *Reason*, November 1994, pp. 48–50.
13. Brian Roehrkasse, quoted in Bloomberg News, "U.S. Need for Data Questioned," *Los Angeles Times*, Jan. 26, 2006, articles.latimes.com/2006/jan/26/business/fi-leahy26, viewed Nov. 22, 2011.
14. In *Brown v. Entertainment Merchants Association*, the Supreme Court decision invalidating California's ban on sale or rental of violent video games to minors, 2011.
15. Passed as Title V of the Telecommunications Act of 1996.
16. *Butler v. Michigan*, 352 U.S. 380(1957).
17. Adjudication on Motions for Preliminary Injunction, *American Civil Liberties Union et al. v. Janet Reno* (No. 96-963) and *American Library Association et al. v. United States Dept. of Justice* (No. 96-1458).
18. *ALA v. United States*.
19. *Brown v. Entertainment Merchants Association.*
20. Brock Meeks, "Internet as Terrorist," *Cyberwire Dispatch*, May 11, 1995, cyberwerks.com/cyberwire/cwd/cwd.95.05.11.htm. Brock Meeks, "Target: Internet," *Communications of the ACM*, August 1995, 38(8), pp. 23–25.
21. The quotations in this paragraph are from Meeks, "Internet as Terrorist."
22. David Armstrong, "Bomb Recipes Flourish Online Despite New Law," *Wall Street Journal*, Jan. 18, 2001, pp. B1, B8. One man accepted a plea bargain for a year in jail.
23. Amol Sharma, "Wireless Carriers Set Strict Decency Standards for Content," *Wall Street Journal*, Apr. 27, 2006, pp. B1, B4.
24. Entertainment Software Ratings Board, www.esrb.org.
25. www.missingkids.com.
26. In the decision striking down the Child Pornography Prevention Act (*Ashcroft v. Free Speech Coalition*). More arguments against the law are in Freedman, "Pondering Pixelized Pixies." Arguments on the other side appear in Foster Robberson, "'Virtual' Child Porn on Net No Less Evil Than Real Thing," *Arizona Republic*, Apr. 28, 2000, p. B11.
27. John Letzing, "'Spam King' Surrenders," *Wall Street Journal*, Aug. 4, 2011, online.wsj.com/article/BT-CO-20110804-726251.html, viewed Nov. 23, 2011.
28. *Intel Corporation v. Hamidi*, news.findlaw.com/wp/docs/intel/intelhamidi63003opn.pdf, viewed Oct. 22, 2011.
29. Jayson Matthews, "Harris Interactive Continues Spam Battle with MAPS," siliconvalley.internet.com/news/article/0,2198,3531_434061,00.html, August 9, 2000, viewed Apr. 9, 2001.
30. Quoted in Tom Espiner, "Antispam Group Rejects E-Mail Payment Plan," CNET News, news.com.com, Feb. 7, 2006, viewed Nov. 27, 2011.
31. The full name is the Controlling the Assault of Non-Solicited Pornography and Marketing Act.
32. Federal Trade Commission, "CAN-SPAM Act: A Compliance Guide for Business," September 2009, business.ftc.gov/documents/bus61-can-spam-act-compliance-guide-business, viewed Oct. 22, 2011.
33. John Simons, "CFTC Regulations on Publishing Are Struck Down," *Wall Street Journal*, June 22, 1999, p. A8. Scott Bullock, "CFTC Surrenders on Licensing Speech," *Liberty & Law*, Institute for Justice, April 2000, 9:2, p. 2.
34. *Swedenburg v. Kelly*.
35. Quoted in Brad Stone, "Web Gurus Aim to Bring Civility to a Bad-Tempered Blogosphere," *New York Times*, Apr. 9, 2007, www.technewsworld.com/story/56774.html, viewed June 21, 2007.
36. A person or organization using the name foia.org leaked the climate research emails. (FOIA is the acronym for "Freedom of Information Act.") I read some (not all) documents at foia2011.org/index.php?id=402. I read numerous articles with quotes from the emails and responses from the CRU researchers. "University of East Anglia Emails: The Most Contentious Quotes," *The Telegraph*, Nov. 23, 2009, www.telegraph.co.uk/earth/environment/

globalwarming/6636563/University-of-East-Anglia-emails-the-most-contentious-quotes.html, viewed Nov. 27, 2011. Antonio Regalado, "Climatic Research Unit Broke British Information Law," *Science*, Jan. 28, 2010, news.sciencemag.org/scienceinsider/2010/01/climate-researc.html, viewed Dec. 23, 2011. Larry Bell, "Climategate II: More Smoking Guns from the Global Warming Establishment," *Forbes*, Nov. 29, 2011, www.forbes.com/sites/larrybell/2011/11/29/climategate-ii-more-smoking-guns-from-the-global-warming-establishment, viewed Dec. 23, 2011. "Cherry-Picked Phrases Explained," University of East Anglia, Nov. 23, 2011, www.uea.ac.uk/mac/comm/media/press/CRUstatements/rebuttalsandcorrections/phrases explained, viewed Dec. 23, 2011.

37. Tim Lister, "WikiLeaks Lists Sites Key to U.S. Security," CNN U.S., Dec. 6, 2010, articles.cnn.com/2010-12-06/us/wikileaks_1_wikileaks-founder-julian-assange-diplomats-homeland-security?_s=PM:US, viewed Aug. 20, 2011. Tim Lister and Emily Smith, "Flood of WikiLeaks Cables Includes Identities of Dozens of Informants," CNN U.S., Aug. 31, 2011, articles.cnn.com/2011-08-31/us/wikileaks.sources_1_diplomatic-cables-wikileaks-websites?_s=PM:US, viewed Oct. 22, 2011.
38. *Die Welt*, quoted in Floyd Abrams, "Don't Cry for Julian Assange," *Wall Street Journal*, Dec. 8, 2011, online.wsj.com/article/SB10001424052970204323904577038293325281030.html, viewed Dec. 26, 2011.
39. *McIntyre v. Ohio Elections Commission*, 514 U.S. 334, 115 S.Ct. 1511 (1995).
40. Jeffrey M. O'Brien, "Free Agent," *Wired*, May 2001, p. 74.
41. Neil King, "Small Start-Up Helps CIA Mask Its Moves on Web," *Wall Street Journal*, Feb. 12, 2001, pp. B1, B6.
42. Declan McCullagh, "SafeWeb's Holes Contradict Claims," *Wired News*, Feb. 12, 2002, www.wired.com/news/politics/0,1283,50371,00.html.
43. Quoted in Robert Corn-Revere, "Caught in the Seamless Web: Does the Internet's Global Reach Justify Less Freedom of Speech?" chapter in Adam Thierer and Clyde Wayne Crews Jr., eds. *Who Rules The Net? Internet Governance and Jurisdiction*, Cato Institute, 2003.
44. Peter L. Bernstein, *Against the Gods: The Remarkable Story of Risk*, John Wiley & Sons, 1996, p. 89.
45. Louisa Lim, "China to Censor Text Messages," BBC News, July 2, 2004, news.bbc.co.uk/2/hi/asia-pacific/3859403.stm.
46. For more on how governments use the Net to thwart freedom movements, see Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom*, PublicAffairs, 2011.
47. Barry Bearak, "Taliban Will Allow Access to Jailed Christian Aid Workers," *New York Times*, Aug. 26, 2001, www.nytimes.com/2001/08/26/world/taliban-will-allow-access-to-jailed-christian-aid-workers.html?pagewanted=all&src=pm, viewed Nov. 26, 2011.
48. In "Google Launches Censored Version of its Search-Engine," Jan. 25, 2006, www.rsf.org.
49. Elinor Mills, "Google to Censor China Web Searches," CNET News.com, Jan. 24, 2006. news.com.com/Google+to+censor+China+Web+searches/2100-1028_3-6030784.htm.
50. Quoted in L. Gordon Crovitz, "Facebook's Dubious New Friends," *Wall Street Journal*, May 2, 2011, online.wsj.com/article/SB10001424052748703567404576293233665299792.html, viewed Nov. 27, 2011.
51. Quoted in Jennifer Valentino-DeVries, Julia Angwin, and Steve Stecklow, "Document Trove Exposes Surveillance Methods," *Wall Street Journal*, Nov. 19, 2011, online.wsj.com/article/SB10001424052970203611404577044192607407780.html, viewed Nov. 26, 2011.
52. "Statement on Temporary Wireless Service Interruption in Select BART Stations on Aug. 11," BART, Aug. 12, 2011, www.bart.gov/news/articles/2011/news20110812.aspx, viewed Oct. 22, 2011. See also Geoffrey A. Fowler, "Phone Cutoff Stirs Worry About Limit on Speech," *Wall Street Journal*, Aug. 16, 2011, online.wsj.com/article/SB10001424053111904253204576510762318054834.html, viewed Oct. 18, 2011.
53. Quoted in Fowler, "Phone Cutoff Stirs Worry."
54. Alan Davidson, "Vint Cerf Speaks Out on Net Neutrality," Google Blog, googleblog.blogspot.com/2005/11/vint-cerf-speaks-out-on-net-neutrality.htm, Nov. 8, 2005.
55. March 2006, quoted on the website of Hands Off the Internet, handsoff.org, viewed July 31, 2006.
56. Armstrong, "Bomb Recipes Flourish Online Despite New Law."
57. Robert D. Atkinson, "Leveling the E-Commerce Playing Field: Ensuring Tax and Regulatory Fairness for Online and Offline Businesses," Progressive Policy Institute, www.ppionline.org, June 30, 2003.
58. Massimo Calabresi, "Quick, Hide the Tanks!" *Time*, May 15, 2000, p. 60.