CHAPTER

3 Networked Communications

Lo, soul, seest thou not God's purpose from the first?
The earth to be spann'd, connected by network,
The races, neighbors, to marry and be given in marriage,
The oceans to be cross'd, the distant brought near,
The lands to be welded together.

–WALT WHITMAN, *Passage to India*

3.1 Introduction

During government meetings in Washington, D.C., it's common for those sitting around the conference table to bow their heads. They're not praying—they're using their smartphones. "You'll have half the participants [texting] each other as a submeeting, with a running commentary on the primary meeting," reports Philippe Reines, a senior advisor to Secretary of State Hillary Clinton [1].

Musician Ken Stringfellow of The Posies uses the Web to interact with his fans. "I log in to Facebook, and in like 30 seconds, I have like 50 people in my chat windows. And I answer their questions: 'Oh, yeah, you wanna get that record? I've got a couple of those in stock.' That kind of stuff" [2].

According to the Pew Research Center, more American adults get their news from the Internet than from newspapers. In a 2008 survey, 40% of adults said they get most

of their news from the Internet, compared to 35% who said they rely upon newspapers as their primary source [3].

The Internet has opened up new opportunities for politicians to attract donations. During his successful run for the Presidency in 2008, Barack Obama raised $500 million from three million donors who contributed over the Internet [4]. A grassroots movement supporting longshot Presidential candidate Ron Paul raised $4 million for him in a single day in 2007 [5].

These stories illustrate how networked communications have become integrated into our lives. Using these networks can be a double-edged sword, however. The Internet and the telephone system efficiently support our desire to interact with other people and accomplish a wide variety of everyday tasks. On other hand, some people use these technologies to lower the quality of our lives through such activities as trying to sell us products we don't want to buy, harassing us, or luring us into wasting our time with frivolous or counterproductive activities.

In this chapter, we explore moral issues associated with our use of the Internet and the telephone system. We begin by focusing on email, the most popular Internet application. After describing how email is routed, we discuss how the increase in unsolicited bulk email, or spam, has degraded the quality of email service.

The World Wide Web has proven to be the most popular way of organizing information on the Internet, and millions of people are using the Web-based social networking service Twitter to communicate with each other. Some governments are threatened by the way in which the Internet has made it so easy for people to access information and communicate with each other. We discuss the different kinds of censorship, the challenges posed to censorship by the Internet, and the morality of censorship.

Next we turn to the issue of freedom of expression. We explore its history in England and the United States, and examine how it became enshrined as the First Amendment to the United States Constitution. While the First Amendment protects freedom of expression, it is not an absolute right. The U.S. Supreme Court has ruled that personal freedom of expression must be balanced against the public good.

To ground our discussion of freedom of expression, we focus on the issue of children and inappropriate content. We discuss how Web filters work, and we summarize the Child Internet Protection Act, which requires Web filters to be installed in public libraries receiving federal funds. We use our set of workable ethical theories to evaluate the morality of this law. At the end of this section, we describe a relatively new phenomenon called sexting, in which children use cell phones to send sexually provocative images of themselves. Sexting provides a good example of how technology has created what James Moor would call a policy vacuum: a situation in which society has not yet determined what should be allowed, what should be forbidden, and what the legal consequences of forbidden actions should be.

The Internet provides new ways to commit fraud and deceive people. Identity thieves are using email and Web sites to capture credit card numbers and other personal information. Pedophiles have used chat rooms to arrange meetings with children. Police have responded to the pedophile threat with "sting" operations, which are them-

selves morally questionable. Web surfers must be aware that the Web contains a great deal of low-quality information. We describe one way in which search engines attempt to direct Web surfers to higher-quality sites.

Some people have used the Internet and/or the telephone network to bully other people. We describe a couple famous instances of cyberbullying and discuss the controversy that has arisen over proposed legislation to ban cyberbullying.

The widespread availability of the Internet has increased the number of people who spend 40 or more hours a week online. Some psychologists claim there are a vast number of Internet addicts. Others say these fears are overblown. In the last section of this chapter we discuss this issue and evaluate the problem of excessive Internet use from an ethical point of view.

3.2 Email and Spam

3.2.1 How Email Works

Email refers to messages embedded in files transferred from one computer to another via a telecommunications system. An email address uniquely indicates a virtual mailbox in cyberspace. Every email address has two parts. The first part (before the `@` sign) identifies the individual user. The second part (after the `@` sign) identifies the domain name. If you are a college student, your college may provide you with an email account, in which case some or all of your domain name is the domain name of your college. Another way to get an email account is through an Internet service provider (ISP). Each ISP has its own domain name.

Suppose you want to send an email to your friend Alyssa Allbright (login name `AA`) at East Dakota State University (domain name `edsu.edu`). You compose the message, indicate the recipient is `AA@edsu.edu`, and send the message. Your mail server uses the domain name system (DNS) to look up `edsu.edu` and find its Internet Protocol (IP) address. This address uniquely identifies a mail server at East Dakota State University. Next, if your email message to Alyssa is more than a few lines long, it is broken up into two or more pieces, called packets. At the front of each packet is the IP address of East Dakota State University.

There is a good chance that your mail server is not directly connected to Alyssa's mail server. The Internet contains thousands of interconnected routers that cooperate to get IP packets to their destination (Figure 3.1). Your server sends the packets to a router that is on the path to East Dakota State. It forwards the packets to the next router on the path, and so on, until the packets arrive at Alyssa's mail server. Her mail server reassembles the packets into an email message and puts it in her mailbox.

3.2.2 The Spam Epidemic

The growth of email has been phenomenal—well over a billion people now have email accounts [6]. Every day about 300 billion email messages are sent. Unfortunately, a significant percentage of this traffic consists of unsolicited bulk email, or spam.

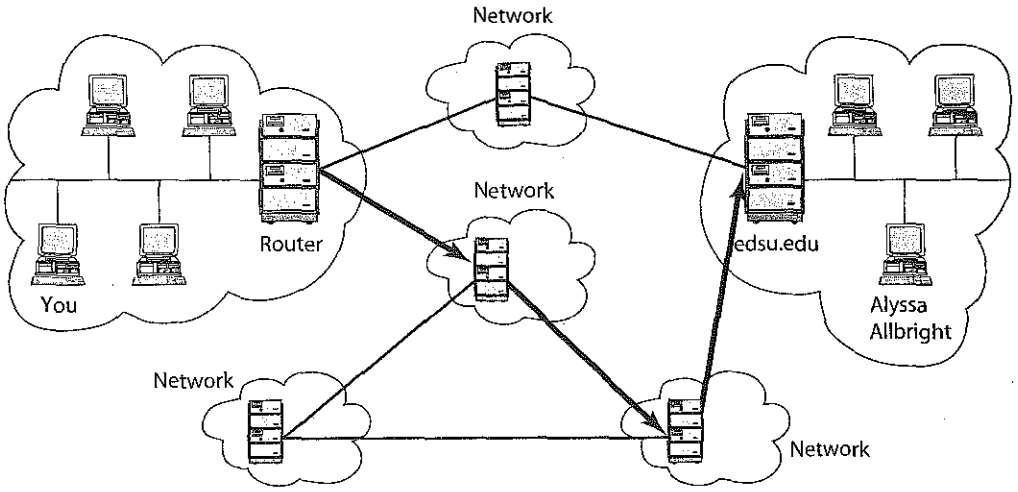


FIGURE 3.1 The Internet connects thousands of local area networks (LANs). Routers pass email and other messages from one LAN to another. Usually there are multiple possible routes.

Why is spam called spam? Brad Templeton, Chairman of the Board of the Electronic Frontier Foundation, traces the term back to the SPAM sketch from *The Final Rip Off* by Monty Python's Flying Circus, in which a group of Vikings drown out a cafe conversation by loudly and obnoxiously repeating the word "spam" [7]. In a similar way, legitimate email messages can get "drowned out" by spam.

The rise of spam corresponds with the transformation of the Internet from a non-commercial academic and research enterprise into a commercial global network. Early spam messages provoked Internet users and generated big headlines. For example, in 1994 Phoenix lawyers Laurence Canter and Martha Siegel sent an email advertising their immigration services to more than 9,000 electronic newsgroups. Canter and Siegel received tens of thousands of responses from outraged newsgroup users who did not appreciate seeing an off-topic, commercial message. *The New York Times* reported the incident with the headline, "An Ad (Gasp!) in Cyberspace." Canter and Siegel were undeterred. Their ad was successful in bringing them new clients. "We will definitely advertise on the Web again," Canter said. "I'm sure other businesses will be advertising on the network in the very near future" [8].

As recently as 2000, spam accounted for only about 8 percent of all email. It was still viewed as a problem for individuals managing their mailboxes. By 2009, about 90 percent of all emails were spam (Figure 3.2) [9]. Today, spam consumes a large percentage of the Internet's bandwidth and huge amounts of storage space on mail servers and individual computers. The cost to businesses is estimated at billions of dollars per year in wasted productivity.

The volume of spam is increasing because spam is effective. The principal advantage of spam is its low cost compared to other forms of advertising. For between $500 and $2,000, a company can send an advertisement to a million different email addresses.

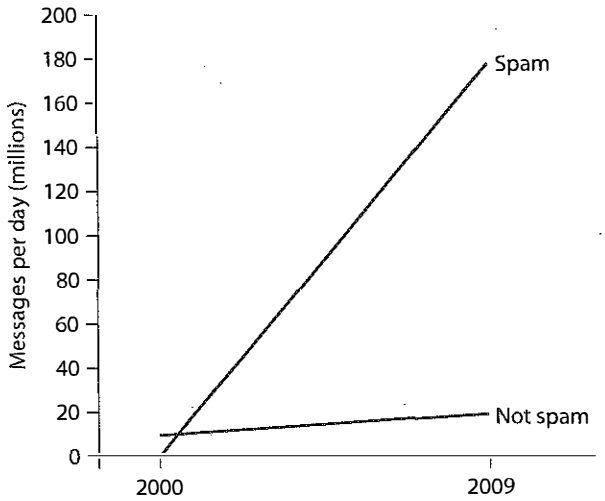


FIGURE 3.2 The increase in spam between 2000 and 2009. In 2000, spam accounted for 8 percent of all email. By 2009, the volume of email had increased 20-fold, and about 90 percent of email messages were spam.

Sending the same advertisement to a million addresses using the U.S. Postal Service costs at least $40,000 for the mailing list and $190,000 for bulk-rate postage. And that doesn't include the cost of the brochures! In other words, an email advertisement is more than 100 times cheaper than a traditional flyer sent out in the mail. The cost is so low that a company can make money even if only one in 100,000 recipients of the spam actually buys the product or service [10].

Where do spammers get email lists with millions of addresses? The Internet provides a variety sources of email addresses that can be harvested and sold to spammers. For example, email addresses often appear in Web sites, in chat-room conversations, and newsgroups. Some computer viruses gather email addresses stored in the address books of PCs and transmit these addresses to spammers.

Another way to garner email addresses is through dictionary attacks (also called directory harvest attacks). Spammers bombard Internet service providers with millions of emails containing made-up addresses, such as AdamA@isprovider.com, AdamB@isprovider.com, AdamC@isprovider.com, and so on. Of course, most of these emails will bounce back, because the addresses are no good. However, if an email *doesn't* bounce, the spammer knows there is a user with that email address and adds it to its mailing list.

Sometimes people voluntarily reveal their email address. Have you ever entered a contest on the Web? There is a good chance the fine print on the entry form said you agree to receive "occasional offers of products you might find valuable" from the company's marketing partners; in other words, spam [10]. Sign-ups for email lists often contain this fine print, too.

How can spammers send out so many email messages? About 90 percent of spam is sent out by bot herders: people who are able to take control of huge networks of

computers. Bot herders create these networks by launching programs that search the Internet for computers with inadequate security and install software robot programs, called bots, on these vulnerable systems. A computer with the bot program installed on it is called a zombie because it can be directed by a remote computer to perform certain tasks. Bot herders can send out billions of email messages every day by dividing the address lists among hundreds of thousands of zombies they control [11].

To deal with this deluge, ISPs install spam filters to block spam from reaching users' mailboxes. These filters look for a large number of messages coming from the same email address, messages with suspicious subject lines, or messages with spam-like content.

Some Internet users have added "challenge-response" software to weed out spam that is not caught by their ISPs. When you send your first email message to one of these users, you'll receive an automated reply, asking you to type in the words or letters appearing in an image. If you respond correctly, the computer knows you're a human, not a bot, and it will allow your email message and all future messages to be delivered. Spam messages, on the other hand, will be blocked [9].

3.2.3 Need for Social–Technical Solutions

As we saw in Chapter 1, new technologies sometimes cause new social situations to emerge. The spam epidemic is an example of this phenomenon. The Internet allows people to send email messages for virtually no cost. Because a spammer's profits increase as the number of sent messages increases, every spammer has an incentive to send as many messages as possible.

The spam problem arose because the Internet and email technology developed without taking social expectations into account. The design of the Internet allows sophisticated users to disguise their own email addresses. Spammers take advantage of this loophole to send out millions of messages, knowing that unhappy recipients will not be able to respond. This is contrary to a fundamental social expectation: fairness. In order to be fair, communications should be two-way, not one-way [12].

3.2.4 Case Study: Ann the Acme Accountant

Ann is an accountant at Acme Corporation, a medium-sized firm with 50 employees. All of the employees work in the same building, and Ann knows all of them on a first-name basis. In fact, Ann distributes paychecks to Acme's employees at the end of every month.

Ann's daughter is a Girl Scout. During the annual Girl Scout cookie sale, Ann sent an email to all of the other Acme employees, inviting them to stop by her desk during a break and place orders. (There is no company rule prohibiting the use of the email system for personal emails.) Nine of the recipients were happy to get Ann's email, and they ordered an average of four boxes of cookies, but the other 40 recipients did not appreciate having to take the time to read and delete an unwanted message; half of them complained to a co-worker about Ann's action.

Did Ann do anything wrong?

KANTIAN ANALYSIS

According to the second formulation of the Categorical Imperative, we should always respect the autonomy of other people, treating them as ends in themselves and never only as the means to an end. The story provides evidence that Ann was not simply "using" her co-workers as the means to her end of making money for the Girl Scouts. She didn't misrepresent what she was doing. She didn't force anyone to buy the cookies or even read the entire email; employees not interested in Girl Scout cookies could simply delete Ann's message as soon as they read the subject line. Some people who received the email freely chose to buy some cookies. Therefore, what Ann did wasn't strictly wrong.

On the other hand, if Ann had found a way for those people interested in hearing about the Girl Scout cookie drive to "opt in" to her announcement, those people not interested in purchasing Girl Scout cookies would not have been bothered by her email. An "opt in" approach would have been better because it would have shown more respect for the autonomy of Ann's co-workers.

ACT UTILITARIAN ANALYSIS

We will do our evaluation in terms of dollars and cents, quantifying the benefits and costs of Ann's action. Let's begin with the benefits. A box of cookies costs $4 and provides $3 of profit to the Girl Scouts. Someone who buys a box of Girl Scout cookies understands it is a fundraising activity and is happy with what he receives for $4. Since the cost of $4 is matched with $4 of benefit, they cancel each other out in our analysis, and we do not have to worry about this factor any more. The average employee who participated in the sale purchased four boxes of cookies. Nine employees participated, which means Ann sold 36 boxes of cookies and provided $108 of benefit to the Girl Scouts.

Now let's look at the harms. The principal harm is going to be the time wasted by Acme's employees. Ann took orders and made deliveries during coffee or lunch breaks, rather than on company time, so our focus is on the 40 employees who did not appreciate getting Ann's solicitation. It's reasonable to assume that they spent an average of 15 seconds reading and deleting the message. That adds up to 10 minutes of lost productivity.

Half of the employees spent 5 minutes complaining about what Ann did with a co-worker. You can imagine the typical conversation. "What makes her so special?" "How does she get away with this kind of thing?" "If I did this for my kid, I'd get in trouble." Taking both the employee's time and the co-worker's time into account, Acme loses 10 minutes of productivity for each conversation. Multiplying 10 minutes by 20 conversations gives us 200 minutes.

The total time wasted equals 210 minutes or 3.5 hours. Assume the average Acme employee makes $20 per hour. The cost of the lost productivity is 3.5 hours times $20 per hour or $70.

The benefit of $108 exceeds the cost of $70, so we may conclude that Ann's action was good. We should note, however, that all of the benefit went to the Girls Scouts and

all of the cost was borne by Acme Corporation. It would be perfectly reasonable if the owners of Acme Corporation concluded that this kind of activity was not in the best interests of the company and created a new policy forbidding the use of company email for cookie drives and other fundraisers.

RULE UTILITARIAN ANALYSIS

What would be the consequences if everyone used the company email system to solicit donations to their favorite causes? All the employees would receive many more messages unrelated to business. There would be plenty of grumbling among employees, lowering morale. Reading and deleting these solicitations would waste people's time, a definite harm. It's unlikely that any one cause would do well if everyone was trying to raise money for his or her own charity. There is a good chance the owner would become aware of this problem, and a logical response would be to ban employees from sending out this kind of solicitation. Because the harms are much greater than the benefits, it is wrong to use the company email system to solicit donations to a charity.

SOCIAL CONTRACT THEORY ANALYSIS

Acme Corporation does not have a prohibition against using the company's email system for personal business. You could say that by sending out her email solicitation, Ann was exercising her right to free speech. Of course, she did it in a way that many people might find obnoxious, because even if they did not choose to read her entire message, they had to take the time to scan the subject line and delete it. Unlike spammers, however, Ann did not disguise her identity as the sender, thereby providing unhappy recipients with the opportunity to respond to her email and voice their disapproval of her solicitation. If many of the 40 people who did not appreciate receiving her email sent a reply communicating their displeasure, then Ann got a taste of her own medicine by having to wade through a bunch of unwanted email messages, and she may choose a better method of advertising the Girls Scout cookie drive next year. From a social contract theory point of view, Ann did nothing wrong.

SUMMARY

Although the analyses of Ann's action from the perspectives of these four ethical theories reached different conclusions, it is clear she could have taken another course of action that would have been much less controversial. Since Ann has only 49 co-workers, it would not have been too difficult for her to find out who wanted to be notified the next time Girl Scouts were selling cookies. She could have put a sign-up sheet on her desk or the company bulletin board, for example. By notifying only those people who signed up, Ann's emails would have been solicited and personal. She could still take advantage of the efficiency of the email system without anyone objecting that she was "using" co-workers or contributing to lost productivity, meaning there would be much less chance of the company instituting a policy forbidding the use of its email system for fundraising activities.

3.3 The World Wide Web

3.3.1 Attributes of the Web

In the past decade the World Wide Web has become the world's most important information storage and retrieval technology. Its creator, Tim Berners-Lee, initially proposed the Web as a documentation system for CERN, the Swiss research center for particle physics, but the creation of easy-to-use Web browsers made the Web accessible to "ordinary" computer users as well [13]. The Web is a hypertext system: a flexible database of information that allows Web pages to be linked to each other in arbitrary fashion.

In Chapter 1 we examined the history of technological innovations that led to the creation of the Web. Here we focus on the attributes that have enabled the Web to become a global tool for information exchange.

1. *It is decentralized.*

   An individual or organization can add new information to the Web without asking for permission from a central authority.

2. *Every object on the Web has a unique address.*

   Any object can link to any other object by referencing its address. A Web object's address is called a **URL** (Uniform Resource Locator).

3. *It is based on the Internet.*

   Building on the Internet makes the Web accessible to people using a wide variety of different computers, such as Macintoshes, Windows systems, or Unix workstations.

The decentralized nature of the Web is one reason why it has grown so rapidly. It also makes the Web more difficult to control. Sometimes the lack of control is viewed as a good thing. For example, the existence of the Web makes it more difficult for an authoritarian government to control the flow of information. On the other hand, the lack of control is sometimes viewed as a weakness. An example of this is when parents attempt to shield their children from Web pages with violent or pornographic content.

3.3.2 How We Use the Web

Web browsers, with their point-and-click navigation and file transfer capabilities, have made the Internet accessible to people with little or no formal computer training. Today, millions of people use the Web for a wide variety of purposes. Here are just a few examples of how people are using the Web.

1. *We shop.*

   The Web enables us to view and order merchandise from the comfort of our homes. Forrester Research predicts that products purchased online in the United States will grow from 6 percent of all retail sales in 2009 to 8 percent in 2014 [14].

2. *We socialize.*

   The Web has become a popular way for friends to keep in touch with each other. The most popular social network is Facebook, with more than 750 million active users in August 2011.

3. *We contribute content.*

   A wiki is a Web site that allows multiple people to contribute and edit its content. The most famous wiki is Wikipedia, an online encyclopedia. Relying on the submissions of hundreds of thousands of volunteers, Wikipedia has become by far the largest encyclopedia in the world. More than three dozen languages are represented by at least 100,000 articles, but by far the most popular language is English, with more than 3.5 million articles written as of 2011. However, critics wonder about the quality of a reference work that allows anyone with a Web browser to contribute [15].

   Other Web sites allow people to upload videos, photos, podcasts, or other digital content. Flickr members can post photos to share with family, friends, or the general public. Reddit combines posting of digital content with an evaluation feature. The most popular submissions rise to the top and are displayed more prominently.

4. *We blog.*

   A blog (short for "Web log") is a personal journal or diary kept on the Web. Used as a verb, the word blog means to maintain such a journal. Blogs may contain plain text, images, audio clips, or video clips [16].

   Some commentators use the term Web 2.0 to refer to a change in the way people use the Web. Social networking services, wikis, Flickr, Reddit, and blogs illustrate that many people are now using the Web not simply to download content, but to build communities and upload and share content they have created.

5. *We learn.*

   In 2001, the Massachusetts Institute of Technology launched its OpenCourseWare program, which has put about 2,000 courses online. Now more than 200 universities from around the globe are partnering with M.I.T. to share course materials on the OpenCourseWare site. These materials are meant to support the independent-learning community rather than replace a traditional university degree [17].

6. *We explore our roots.*

   In the past, genealogists interested in accessing American immigration and census records had the choice between mailing in their requests and waiting for them to be processed or visiting the National Archives and examining the documents by hand. Now that the National Archives has put more than 50 million historical records online, the same searches can be performed remotely—and much more quickly—over the Internet (Figure 3.3) [18].

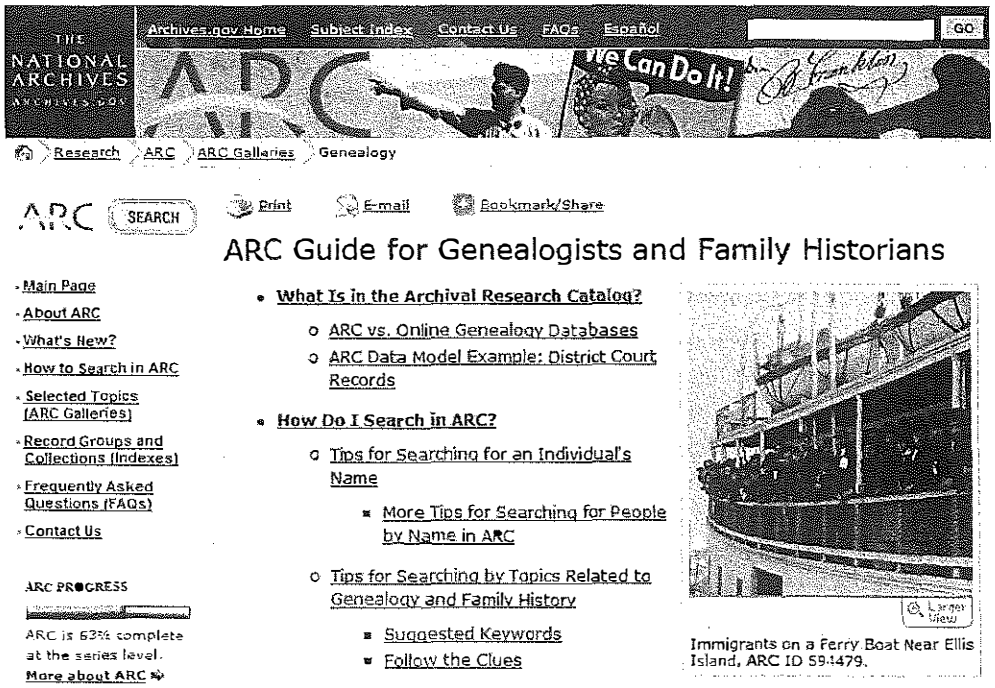


FIGURE 3.3 The U.S. National Archives and Records Administration has simplified the work of genealogists by putting millions of records online.

7. *We enter virtual worlds.*

An online game is a game played on a computer network that supports the simultaneous participation of multiple players. A persistent online game is an online game in which each player assumes the role of a character in a virtual world and the attributes of the character and the world persist beyond a single gaming session. The most popular persistent online game is *World of Warcraft*, with more than ten million monthly subscribers worldwide [19]. At times, the number of simultaneous players in China alone has reached one million [20].

Another hub of persistent online gaming is South Korea. Cybercafés (called PC bangs in South Korea) have large-screen monitors enabling spectators to watch the gameplay, which is full of virtual violence and mayhem. Some children spend up to 10 hours a day playing games, hoping to turn professional. Kim Hyun Soo, chairman of the Net Addiction Treatment Center, complains that "young people are losing their ability to relate to each other, except through games" [21]. We'll discuss the topic of Internet addiction in Section 3.8.

The phenomenon of global online gaming has created a real economy based on virtual worlds. Some people are making a living playing persistent online games. Chinese "gold farmers" who work 12 hours a day, 7 days a week can earn $3,000 a year killing monsters, harvesting virtual gold coins and artifacts, creating powerful avatars, and selling them over the Internet [22].

8. *We pay our taxes.*

   Millions of Americans now file their federal income taxes through the Internal Revenue Service's Web site [23].

9. *We gamble.*

   Internet gambling is a $20-billion-a-year global business [24]. Running an Internet-based casino is illegal in most states. As a result, many American emigrés are operating gambling Web sites from the Caribbean or Central America [25].

10. *We take humanitarian action.*

    Kiva is Web site supporting person-to-person micro-lending. Kiva works with microfinance institutions to identify entrepreneurs from poor communities, and it posts information about these entrepreneurs on its Web site. People who wish to make an interest-free loan are able to identify the particular person to whom they would like to lend money. Lenders have the ability to communicate with the entrepreneurs and see the impact their loans are having on the recipients, their families, and their communities [26].

3.3.3 Twitter

Twitter is a Web-based social networking service that allows its users to send out text messages known as tweets. Tweets are limited to 140 characters because that's the maximum length of a cell phone text message. The service is popular because people who want their friends to know what they are doing find it more convenient to post a single tweet than to type a bunch of text messages. Many people also use Twitter as a blogging tool; they make their tweets public so that anyone can read them. Other Twitter members never post tweets, but they sign up to follow the tweets posted by other people they are interested in.

More than 200 million people use Twitter, making it one of the most popular Web services in the world [27]. Users posted 7,196 tweets per second at the conclusion of the exciting World Cup final soccer match between the United States and Japan in 2011 [28].

BUSINESS PROMOTION

When carpenter Curtis Kimball started a part-time business running a crème brûlée cart in San Francisco, he used Twitter to let people know the cart's location and the flavors of the day. Before long, he had attracted 5,400 followers. Business became so good he quit his day job in order to keep up with demand. Many tiny businesses with no money for advertising rely upon Twitter as their only marketing tool [29].

ARAB SPRING UPRISINGS

Twitter and Facebook played a highly visible role in the "Arab Spring" demonstrations in 2011 that led to revolutions in Tunisia and Egypt, a civil war in Libya, and protests in many other Arab countries. In the midst of the protests in Cairo that led to the resignation of President Hosni Murbarak, one protester tweeted: "We use Facebook to

schedule the protests, Twitter to coordinate, and YouTube to tell the world" [30]. Arab news organization Al Jazeera has created a "Twitter Dashboard" indicating the level of tweeting activity in many Arab nations where there has been unrest [31].

Scholars of the Arab Spring uprisings point to an interesting phenomenon: People started using online social networks such as Twitter in order to keep up with their friends, but these interactions caused them to become politicized. Through these networks, bloggers met new people, became exposed to new ideas, and developed an interest in human rights [32].

Others think the role of social media in catalyzing social change has been overblown. They argue that social networks like Twitter and Facebook are great at building networks of people with weak connections to each other, but high-risk activism requires strong ties among the members of a hierarchical organization [33].

3.3.4 Too Much Governmental Control or Too Little?

The University of Toronto, Harvard Law School, the University of Cambridge, and Oxford University formed the OpenNet Initiative to research Internet filtering and surveillance around the world [34]. Their research has revealed that the level of filtering by governments has increased rapidly in the past few years. Governments limit access to the Internet in a variety of ways.

One approach is to make the Internet virtually inaccessible. The governments of Burma (Myanmar), Cuba, and North Korea make it difficult for ordinary citizens to use the Internet to communicate with the rest of the world [35, 36, 37].

In other countries, Internet access is easier, but still carefully controlled. Saudi Arabians gained access to the Internet in 1999, after the government installed a centralized control center outside Riyadh. Virtually all Internet traffic flows through this control center, which blocks pornography sites, gambling sites, and many other pages deemed to be offensive to Islam or the government of Saudi Arabia [38]. Blocked sites and pages are from such diverse categories as Christian evangelism, women's health and sexuality issues, music and movies, gay rights, Middle Eastern politics, and information about ways to circumvent Web filtering.

The Chinese government has blocked access to the Internet during times of social unrest. For example, in July 2009, China responded to ethnic riots in the autonomous region of Xinjiang by turning off Internet service to the entire region for ten months [39, 40].

China has also built one of the world's most sophisticated Web filtering systems [41]. The Great Firewall of China prevents Chinese citizens from accessing certain Internet content by blocking messages coming from blacklisted sites. The government employs human censors to identify sites that should be blacklisted [42]. Among the Web sites blacklisted by the government include those containing pornography, those associated with the Dalai Lama or the Falun Gong, those referring to the 1989 military crackdown, and those run by certain news organizations, such as Voice of America and

BBC News. Before the 2008 Summer Olympics, the International Olympic Committee assured journalists that they would have unfettered access to the Internet during their stay in Beijing, but once the journalists arrived in Beijing, they discovered that many sites were blocked. The International Olympic Committee admitted that it had agreed to allow to be blocked sensitive sites "not considered Games related" [43].

Some contend that blogs and nongovernmental Web sites are eroding the Chinese government's ability to restrict the communications of its citizens [42], but the government has not given up. The government continues to shut down Web sites and censor blogs that it finds contrary to the interests of the state. In May 2009, the government told all PC makers that they would need to install Web-content filtering software on all PCs sold in China beginning July 1, 2009. The software, called Green Dam/Youth Escort, is designed to prevent a Web browser from displaying Web pages from blacklisted sites. As the government updated its list of banned sites, computers would automatically download the updated lists. The proposal did not sit well with many Chinese citizens, who protested the decision on blogs and social networking sites. They argued that although the government claimed the software would be used only to block access to pornographic Web sites, its real use would be to block politically sensitive sites. Computer experts critized the Green Dam/Youth Escort software for making personal computers vulnerable to intrusions from hackers. At the end of June 2009, the Chinese government declared that it was delaying—but not cancelling—the requirement that all new PCs come equipped with Green Dam/Youth Escort software [44, 45, 46]. In August 2009, the government retreated further, stating that while public computers in schools and Internet cafes must run Green Dam/Youth Escort, its use among private computer owners would be voluntary [47].

Meanwhile, Western nations have different standards about what is acceptable and what is not. For example, Germany forbids access to any neo-Nazi Web site, but Web surfers in the United States can access many such sites.

Political satire and pornography are easily available through American ISPs. Americans are used to political satire, but many citizens are concerned about the corrupting influence of pornography, particularly with respect to minors. Since 1996 the U.S. Congress has passed three laws aimed at restricting access of children to sexually explicit materials on the Web: the Communications Decency Act, the Child Online Protection Act, and the Children's Internet Protection Act. The first two laws were ruled unconstitutional by the U.S. Supreme Court; the third was upheld by the Supreme Court in June 2003.

3.4 Censorship

Censorship is the attempt to suppress or regulate public access to material considered offensive or harmful. Historically, most censorship has been exercised by governments and religious institutions. For example, Roman censors banished the poets Ovid and Juvenal for their writings. During the Middle Ages the Inquisition suppressed the publication of many books, including the work of Galileo Galilei.

Censorship became a much more complicated issue with the invention of the printing press. The printing press broke the virtual monopoly held by governments and religious institutions on distributing material to a large audience, and the increase in printed material increased the number of literate people. For the first time, private individuals could broadcast their ideas to others on a wide scale.

In Western democracies, the gradual separation of church and state has left the government as the sole institution responsible for censorship. In other parts of the world, such as the Middle East, religious institutions continue to play a significant role in determining which material should be accessible to the public.

3.4.1 Direct Censorship

Direct censorship has three forms: government monopolization, prepublication review, and licensing and registration.

The first form of direct censorship is government monopolization. In the former Soviet Union, for example, the government owned all the television stations, radio stations, and newspapers. Private organizations could not even own a photocopy machine. Government monopolization is an effective way to suppress the flow of information. Modern computer and communication technology makes government monopolization much more difficult than it has been in the past.

Prepublication review is the second form of direct censorship. This form of censorship is essential for material the government wishes to keep secret, such as information about its nuclear weapons program. Most governments have laws restricting the publication of information that would harm the national security. In addition, autocratic governments typically block publication of material deemed injurious to the reputations of their rulers.

The third form of direct censorship is licensing and registration. This form of censorship is typically used to control media with limited bandwidth. For example, there are a limited number of radio and television stations that can be accommodated on the electromagnetic spectrum. Hence a radio or television station must obtain a license to broadcast at a particular frequency. Licensing invites censorship. For example, the U.S. Federal Communications Commission has banned the use of certain four-letter words. This led to a challenge that went all the way to the U.S. Supreme Court, as we will see in Section 3.5.3.

3.4.2 Self-Censorship

Perhaps the most common form of censorship is self-censorship: a group deciding for itself not to publish material. In some countries a publisher may censor itself in order to avoid persecution. For example, after U.S.-led forces toppled the regime of Saddam Hussein in April 2003, CNN's chief news executive Eason Jordan admitted that CNN had suppressed negative information about the actions of the Iraqi government for more than a decade in order to keep CNN's Baghdad bureau open and protect Iraqi employees of CNN [48].

In other countries, publishers may want to maintain good relations with government officials. Publications compete with each other for access to information. Often this information is available only from government sources. Publishers know that if they offend the government, their reporters may not be given access to as much information as reporters for rival publications, putting them at a competitive disadvantage. This knowledge can lead a "free" press to censor itself.

Publishers have adopted ratings systems as a way of helping people decide if they (or their children) should access particular offerings. For example, television stations in the United States broadcast shows with "mature content" late in the evening. Voluntary rating systems help people decide if they (or their children) will see a movie, watch a television show, or listen to a CD.

The Web does not have a universally accepted ratings system. Some Web sites practice a form of labeling. For example, the home page may warn the user that the site contains nudity and require the user to click on an "I agree" button to enter the site. However, other sites have no such warnings. People who stumble onto these sites are immediately confronted with images and text they may find offensive.

3.4.3 Challenges Posed by the Internet

Five characteristics of the Internet make censorship more difficult:

1. *Unlike traditional one-to-many broadcast media, the Internet supports many-to-many communications.*

   While it is relatively easy for a government to shut down a newspaper or a radio station, it is very difficult for a government to prevent an idea from being published on the Internet, where millions of people have the ability to post Web pages.

2. *The Internet is dynamic.*

   Millions of new computers are being connected to the Internet each year.

3. *The Internet is huge.*

   There is simply no way for a team of human censors to keep track of everything that is posted on the Web. While automated tools are available, they are fallible. Hence, any attempt to control access to material stored on the Internet cannot be 100 percent effective.

4. *The Internet is global.*

   National governments have limited authority to restrict activities happening outside their borders.

5. *It is hard to distinguish between children and adults on the Internet.*

   How can an "adult" Web site verify the age of someone attempting to enter the site?

3.4.4 Ethical Perspectives on Censorship

KANT'S VIEWS ON CENSORSHIP

As a thinker in the tradition of the Enlightenment, Kant's motto was, "Have courage to use your own reason" [49]. Kant asks the rhetorical question, "Why don't people

think for themselves?" and answers it: "Laziness and cowardice are the reasons why so great a portion of mankind, after nature has long since discharged them from external direction, nevertheless remain under lifelong tutelage, and why it is so easy for others to set themselves up as their guardians. It is so easy not to be of age. If I have a book which understands for me, a pastor who has a conscience for me, a physician who decides my diet, and so forth, I need not trouble myself. I need not think, if I can only pay—others will readily undertake the irksome work for me" [49].

The Enlightenment was a reaction to the institutional control over thought held by the aristocracy and the Church. Kant believed he was living in a time in which the obstacles preventing people from exercising their own reason were being removed. He opposed censorship as a backward step.

MILL'S VIEWS ON CENSORSHIP

John Stuart Mill also championed freedom of expression. He gave four reasons why freedom of opinion, and freedom of expression of opinion, were necessary.

First, none of us is infallible. All of us are capable of error. If we prevent someone from voicing their opinion, we may actually be silencing the voice of truth.

Second, while the opinion expressed by someone may be erroneous, it may yet contain a kernel of truth. In general, the majority opinion is not the whole truth. We ought to let all opinions be voiced so that all parts of the truth are heard.

Third, even if the majority opinion should happen to be the whole truth, it is in the clash of ideas that this truth is rationally tested and validated. The whole truth left untested is simply a prejudice.

Fourth, an opinion that has been tested in the fire of a free and open discourse is more likely to have a "vital effect on the character and conduct" [50].

Therefore, Mill, like Kant, fundamentally supported the free exchange of ideas with the conviction that good ideas would prevail over bad ones. Applying their philosophy to the World Wide Web, it seems they would support the free exchange of opinions and oppose any kind of government censorship of opinions.

MILL'S PRINCIPLE OF HARM

However, a lack of government censorship can also lead to harm. Under what circumstances should the government intervene? Mill proposed the principle of harm as a way of deciding when an institution should intervene in the conduct of an individual.

PRINCIPLE OF HARM

"The only ground on which intervention is justified is to prevent harm to others; the individual's own good is not a sufficient condition" [50].

In other words, the government should not get involved in the private activities of individuals, even if the individuals are doing something to harm themselves. Only if individuals' activities are harming other people should the government step in.

The principle of harm can be used to explain the position of most Western democratic governments with respect to censoring pornographic material depicting adults. Some ethicists conclude it is not wrong for adults to view pornography depicting adults. Others hold that this activity is immoral. If the activity is immoral, it is more certain the harm is being done to the individual consumer; less certain is how much harm is being done to other people. Hence, the principle of harm can be used as an argument why the government should not be trying to prevent adults from using pornography depicting adults.

3.5 Freedom of Expression

In the United States, freedom of expression is one of the most cherished—and most controversial—rights. In this section, we explain the history behind the adoption of the First Amendment to the United States Constitution. We also explore why the freedom of expression has not been treated as an absolute right.

3.5.1 History

At the time of the American Revolution, any criticism of government was seen as a threat to public order and could result in fines and/or imprisonment. Restrictions on freedom of speech in England date back to 1275 and a law called De Scandalis Magnatum. According to this law, a person could be imprisoned for spreading stories about the King that could have the effect of weakening the loyalty of his subjects. The scope of the law became much broader through numerous revisions over the next two centuries. Eventually it encompassed seditious words and words spoken against a wide variety of government officials, including justices [51].

The De Scandalis Magnatum was administered by the Court of Star Chamber, or "Star Chamber" for short. The Star Chamber reported directly to the King, and it did not have to obey traditional rules of evidence. Rulings of the Star Chamber demonstrated that a person could be convicted for making a verbal insult or for something written in a private letter. The Star Chamber was abolished in 1641, but the law continued to be enforced through Common Law Courts [51].

At the end of the eighteenth century, freedom of the press in England and its colonies meant freedom to print without a license. In other words, there were no prior restraints on publication. People could publish what they pleased. However, those who published material found to be seditious or libelous would face severe consequences [51].

The law against libel simply considered if the material printed was harmful; arguing that the information was true was not relevant to the proceedings and could not be used in a publisher's defense. Between 1760 and the end of the American Revolution, about 50 people were successfully prosecuted for libel. To prevent such prosecutions from continuing, most states adopted bills of rights after gaining independence from England [51].

In May 1787, delegates from the thirteen states gathered in Philadelphia to revise the Articles of Confederation. Soon they were drafting a completely new Constitution. Delegate George Mason, author of the Virginia Declaration of Rights, strongly opposed the proposed Constitution because it contained no declaration of the rights of the citizens. Patrick Henry and other political leaders shared Mason's objections [51].

While the proposed Constitution was ratified by all thirteen states, most state legislatures adopted the Constitution with the expectation that Congress would offer amendments addressing the human rights concerns brought up by the opponents of the Constitution. During the first Congress, James Madison proposed 12 such amendments. All 12 of these amendments were sent to the states for ratification. Of these 12 amendments, 10 were quickly ratified. Today, these 10 amendments are commonly known as the Bill of Rights. The first of these amendments, the one Madison considered most essential, was the one guaranteeing freedom of speech and freedom of the press [51].

FIRST AMENDMENT TO THE UNITED STATES CONSTITUTION

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

3.5.2 Freedom of Expression Not an Absolute Right

The primary purpose of the First Amendment's free speech guarantee is political. Free speech allows an open discussion of public issues. It helps make government responsive to the will of the people [52].

However, the First Amendment right to free expression is not limited to political speech. Nonpolitical speech is also covered (Figure 3.4). There are good reasons for protecting nonpolitical as well as political speech. First, it is sometimes hard to draw the line between the two. Asking a judge to make the distinction turns it into a political decision. Second, society can benefit from nonpolitical as well as political speech. Hence, the free speech guarantee of the First Amendment also promotes scientific and artistic expression. For the same reason, the definition of "speech" encompasses more than words. Protected "speech" includes art and certain kinds of conduct, such as burning an American flag [53].

Decisions by the U.S. Supreme Court have made clear that freedom of expression is not an absolute right. Instead, the private right to freedom of expression must be balanced against the public good. Those who abuse this freedom and harm the public may be punished. For example, protection is not given to "libel, reckless or calculated lies, slander, misrepresentation, perjury, false advertising, obscenity and profanity, solicitation of crime, and personal abuse or 'fighting' words," because these actions do not serve the ends of the First Amendment [52].

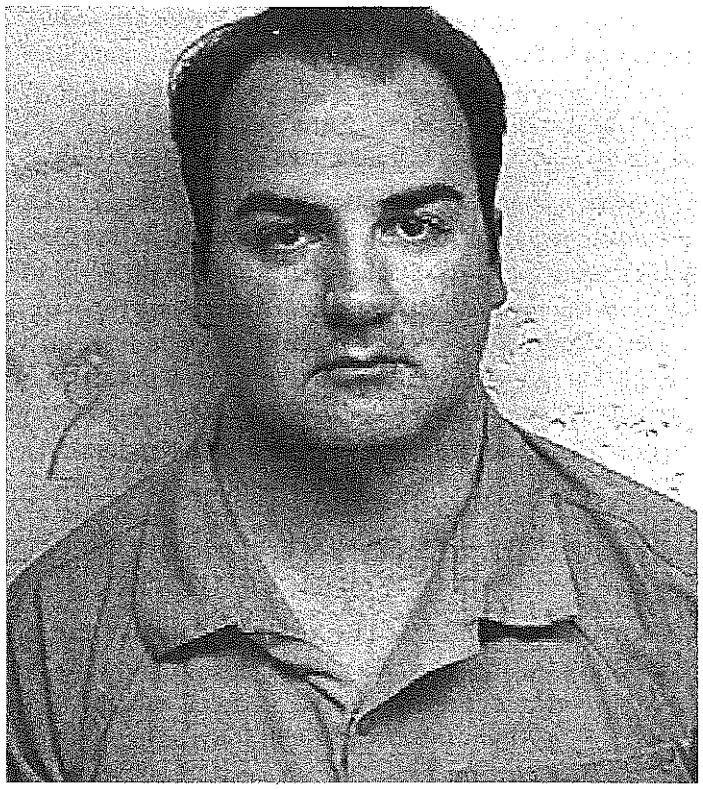


FIGURE 3.4 Jeremy Jaynes was convicted under Virginia law for sending millions of spam messages. His conviction was overturned by the Supreme Court of Virginia because the anti-spam law was too broad and also prohibited the anonymous transmission of unsolicited bulk emails "containing political, religious or other speech protected by the First Amendment to the United States Constitution" [54]. (AP Photo/Loudoun County Sheriff's office)

Various restrictions on freedom of speech are justified because of the greater public good that results. For example, U.S. law prohibits cigarette advertising on television because cigarette smoking has detrimental effects on public health. Some cities use zoning laws to concentrate adult bookstores in a single part of town because the presence of adult bookstores lowers property values and increases crime.

3.5.3 *FCC v. Pacifica Foundation et al.*

To illustrate limits to First Amendment protections, we consider the decision of the U.S. Supreme Court in the case of *Federal Communications Commission v. Pacifica Foundation et al.*

In 1973, George Carlin recorded a performance made in front of a live audience in California. One track on the resulting record is a 12-minute monologue called "Filthy Words." In the monologue Carlin lists seven words that "you couldn't say on the public, ah, airwaves, um, the ones you definitely wouldn't say, ever" [55]. The audience laughs as

Carlin spends the rest of the monologue creating colloquialisms from the list of banned words.

On the afternoon of October 30, 1973, counterculture radio station WBAI in New York aired "Filthy Words" after warning listeners the monologue contained "sensitive language which might be regarded as offensive to some" [56]. A few weeks after the broadcast, the Federal Communications Commission (FCC) received a complaint from a man who had heard the broadcast on his car radio in the presence of his son. In response to this complaint, the FCC issued a declaratory order and informed Pacifica Foundation (the operator of WBAI) that the order would be placed in the station's license file. The FCC warned Pacifica Foundation that further complaints could lead to sanctions.

Pacifica sued the FCC, and the resulting legal battle reached the U.S. Supreme Court. In 1978, the Supreme Court ruled, in a 5–4 decision, that the FCC did not violate the First Amendment [56]. The majority opinion states, "[O]f all forms of communication, it is broadcasting that has received the most limited First Amendment protection." There are two reasons why broadcasters have less protection than book sellers or theater owners:

1. *"Broadcast media have a uniquely pervasive presence in the lives of all Americans."*

   Offensive, indecent material is broadcast into the privacy of citizens' homes. Since people can change stations or turn their radios on or off at any time, prior warnings cannot completely protect people from being exposed to offensive material. While someone may turn off the radio after hearing something indecent, that does not undo a harm that has already occurred.

2. *"Broadcasting is uniquely accessible to children, even those too young to read."*

   In contrast, restricting children's access to offensive or indecent material is possible in bookstores and movie theaters.

The majority emphasized that its ruling was a narrow one and that the context of the broadcast was all-important. The time of day at which the broadcast occurred (2 p.m.) was an important consideration, because that affected the composition of the listening audience.

3.5.4 Case Study: Kate's Blog

Kate is a journalism major who maintains a popular blog focusing on campus life. Kate attends a private birthday party in someone's apartment for her friend Jerry, a college student active in the Whig Party on campus. Someone gives Jerry a Tory Party T-shirt as a gag gift, and Jerry puts it on. Kate uses her cell phone to get a picture of Jerry wearing the T-shirt when he is looking the other way. She posts the photo on her blog without asking him permission. In the blog she identifies Jerry and explains the context in which the photo was taken.

The story is read by many people both on and off campus. The next day, Jerry confronts Kate, yells at her for posting the photo, and demands that she remove it from

her Web site. Kate complies with Jerry's request by removing the photo, and the two of them remain friends. As a result of the incident, Jerry becomes more popular on campus, and the number of people who read Kate's blog increases.

Was it wrong for Kate to post the picture of Jerry on her blog without first getting his permission?

KANTIAN ANALYSIS

By uploading Jerry's photo to her blog without first asking his permission, Kate didn't respect Jerry's autonomy. Instead, she treated him as a means to her end of increasing the readership of her Web site. Therefore, her action was wrong according to the second formulation of the Categorical Imperative.

SOCIAL CONTRACT THEORY ANALYSIS

The birthday party was held in the apartment of one of Jerry's friends. In this private setting and among friends Jerry had a legitimate expectation that what happened during the party would not be broadcast to the world. By secretly taking a photo of Jerry doing something out of character and posting that photo on her blog, Kate violated Jerry's right to privacy. For this reason Kate's action was wrong.

ACT UTILITARIAN ANALYSIS

We need to determine the positive and negative consequences of Kate's action on the two people involved. Kate increased the popularity of her blog, which is precisely the positive outcome she wanted. Jerry's anger at Kate shows that he was hurt and upset by what she did, but after he confronted her, she removed the photo from her Web site and they reconciled. Therefore, while the intensity of this negative consequence to Jerry was intense, its duration was brief. As a result of the posting, Jerry became more popular on campus, a very good thing for someone active in campus politics. Jerry had Kate to thank for this boost in his popularity, further quenching the unhappiness he initially felt when he learned what she had done. We conclude that the short-term consequences for both Kate and Jerry were positive.

The long-term consequences are difficult to determine. It is possible that the photo could land in the wrong hands and be used to discredit Jerry some day in the future, but this would depend on many factors. Jerry is currently politically active. Is he going to stay active in Whig politics after he graduates from college? The photo was only on the Web for a day. Did anyone download it? If so, what is the chance that some day the photo will fall into the hands of someone who wants to make Jerry look bad?

An important part of a utilitarian analysis is looking at the certainty of each consequence: in other words, the probability that it will happen. The short-term consequences of Kate's action are certainly positive for both Kate and Jerry. The long-term negative consequences, if any, are not certain at all. We conclude Kate did nothing wrong by posting Jerry's photo on her blog.

RULE UTILITARIAN ANALYSIS

Let's consider what would happen if everyone were constantly taking photos of everyone they bumped into and posting them on the Web. There would be some positive consequences. It would be easier for people to see what their friends were up to. People might be more reluctant to engage in illegal activities if they thought photo or video evidence might appear on the Web. There would also be a variety of negative consequences. Once people started to feel as if they were always being photographed, they would become self-conscious, making it more difficult for them to simply be themselves. People would be less free to take off their public persona and express their true feelings. Inevitably people would post photos that caused hard feelings and led to strained relationships. Ultimately, the negative consequences seem to be more weighty than the positive consequences, and we conclude Kate's action was wrong.

SUMMARY

The analyses from the perspectives of Kantianism, social contract theory, and rule utilitarianism all conclude it was wrong for Kate to post the photo without asking Jerry's permission, though each analysis uses a different line of reasoning to reach that conclusion. Kate imagined (correctly, as it turns out) that Jerry would be angry if she took a photo of him wearing the Tory Party T-shirt, and that is why she took the photo when he wasn't looking. Kate figured it would be better to beg for forgiveness than ask for permission, but what she did was cut Jerry out of a decision that affected both of them. This is no way to treat anybody, much less a friend. Kate would have been better off trying to persuade Jerry that putting the photo on her blog would be to their mutual advantage, posting the image only after obtaining his consent.

3.6 Children and Inappropriate Content

Many parents and guardians believe they ought to protect their children from exposure to pornographic and violent materials. A few years ago, the center of concern was the Web, and a large software industry sprang up to provide browsers with the ability to block inappropriate images. Now, camera-equipped cell phones are becoming commonplace, and some parents are being forced to confront the unpleasant reality that their children have emailed sexually provocative images of themselves to friends or even strangers.

3.6.1 Web Filters

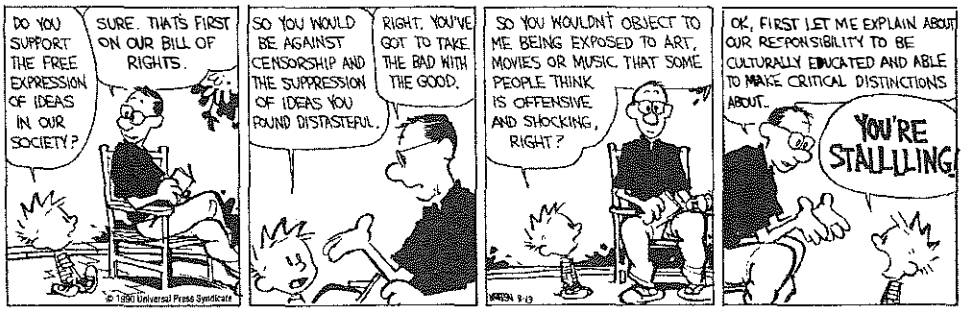
A Web filter is a piece of software that prevents certain Web pages from being displayed by your browser. While you are running your browser, the filter runs as a background process, checking every page your browser attempts to load. If the filter determines that the page is objectionable, it prevents the browser from displaying it.

Filters can be installed on individual computers, or an ISP may provide filtering services for its customers. Programs designed to be installed on individual computers, such as Cyber Sentinel, eBlaster, and Spector PRO, can be set up to email parents as soon

as they detect an inappropriate Web page [57]. America Online's filtering service is called AOL Guardian. It enables parents to set the level of filtering on their children's accounts. It also allows parents to look at logs showing the pages their children have visited.

Typical filters use two different methods to determine if a page should be blocked. The first method is to check the URL of the page against a "blacklist" of objectionable sites. If the Web page comes from a blacklisted site, it is not displayed. The second method is to look for combinations of letters or words that may indicate a site has objectionable content.

Neither of these methods is foolproof. The Web contains millions of pages containing pornography, and new sites continue to be created at a high rate, so any blacklist of pornographic sites will be incomplete by definition. Some filters sponsored by conservative groups have blacklisted sites associated with liberal political causes, such as those sponsored by the National Organization of Women and gay and lesbian groups. The algorithms used to identify objectionable words and phrases can cause Web filters to block out legitimate Web pages.



CALVIN AND HOBBES © 1990 Watterson. Dist. By UNIVERSAL UCLICK.
Reprinted with permission. All rights reserved.

3.6.2 Child Internet Protection Act

In March 2003, the Supreme Court weighed testimony in the case of *United States v. American Library Association*. The question: Can the government require libraries to install antipornography filters in return for receiving federal funds for Internet access?

More than 14 million people access the Internet through public library computers. About one-sixth of the libraries in the United States have already installed filtering software on at least some of their computers. The Child Internet Protection Act requires that libraries receiving federal funds to provide Internet access to its patrons must prevent children from getting access to visual depictions of obscenity and child pornography. The law allows adults who desire access to a blocked page to ask a librarian to remove the filter.

In his testimony before the Supreme Court, Solicitor General Theodore Olson argued that since libraries don't offer patrons X-rated magazines or movies, they should not be obliged to give them access to pornography over the Internet.

Paul Smith, representing the American Library Association and the American Civil Liberties Union, argued that in their attempt to screen out pornography, filters block

tens of thousands of inoffensive pages. He added that requiring adults to leave the workstation, find a librarian, and ask for the filter to be turned off would be disruptive to their research and would stigmatize them.

In June 2003, the U.S. Supreme Court upheld CIPA, ruling 6–3 that anti-pornography filters do not violate First Amendment guarantees [58]. Chief Justice William Rehnquist wrote, "A public library does not acquire Internet terminals in order to create a public forum for Web publishers to express themselves, any more than it collects books in order to provide a public forum for the authors of books to speak . . . Most libraries already exclude pornography from their print collections because they deem it inappropriate for inclusion" [59].

3.6.3 Ethical Evaluations of CIPA

In this section, we evaluate CIPA from the perspectives of Kantianism, act utilitarianism, and social contract theory.

KANTIAN EVALUATION

We have already covered Kant's philosophical position against censorship. He optimistically believed that allowing people to use their own reason would lead to society's gradual enlightenment. In this case, however, the focus is narrower. Rather than talking about censorship in general, let's look at CIPA in particular.

The goal of CIPA is to protect children from the harm caused by exposure to pornography. The way the goal is being implemented is through Web filters. Studies have demonstrated that Web filters do not block all pornographic material, but do block some nonpornographic Web pages. Some nonpornographic information posted on the Web will not be easily accessible at libraries implementing government-mandated Web filters. The people posting this information did not consent to their ideas being blocked. Hence, the decision to require the use of Web filters treats the creators of non-offensive but blocked Web pages solely as means to the end of restricting children's access to pornographic materials. This analysis leads us to conclude that CIPA is wrong.

ACT UTILITARIAN EVALUATION

Our second evaluation of CIPA is from an act utilitarian point of view. What are the consequences of passing CIPA?

1. While not all children access the Web in public libraries, and while Web filtering software is imperfect, it is probable that enacting CIPA will result in fewer children being exposed to pornography, which is good.
2. Because Web filters are imperfect, people will be unable to access some legitimate Web sites. As a result, Web browsers in libraries will be less useful as research tools, a harmful consequence.
3. Adult patrons who ask for filters to be removed may be stigmatized (rightfully or not) as people who want to view pornography, a harm to them.
4. Some blocked sites may be associated with minority political views, reducing freedom of thought and expression, which is harmful.

Whenever we perform the utilitarian calculus and find some benefits and some harms, we must decide how to weigh them. This is a good time to think about utilitarian philosopher Jeremy Bentham's seven attributes. In particular, how many people are in each affected group? What is the probability the good or bad event will actually happen? How soon is the event likely to occur? How intense will the experience be? To what extent is the pain not diluted by pleasure, or vice versa? How long will it last? How likely is the experience to lead to a similar experience? Actually performing the calculus for CIPA is up to each person's judgment. Different people could reach opposite conclusions about whether enacting CIPA is the right thing for the U.S. government to do.

SOCIAL CONTRACT THEORY EVALUATION

In social contract theory, morally binding rules are those rules mutually agreed to in order to allow social living [60]. Freedom of thought and expression is prized. According to John Rawls, "liberty of conscience is to be limited only when there is a reasonable expectation that not doing so will damage the public order which the government should maintain" [61].

It would be difficult to gain consensus around the idea that the private viewing of pornography makes social living no longer possible. For this reason, the private use of pornography is considered to be outside the social contract and nobody else's business. However, when we think about the availability of pornography in public libraries, the issue gets thornier.

Some argue that allowing people to view pornography in a public place demeans women, denying them dignity as equal persons [62]. On the other hand, we know that filtering software is imperfect. In the past it has been used to promote a conservative political agenda by blocking sites associated with other viewpoints [63, 64]. Hence it reduces the free exchange of ideas, limiting the freedoms of thought and expression. For some adults, public libraries represent their only opportunity to access the Web for no cost. In order to be treated as free and equal citizens, they should have the same Web access as people who have Internet access from their homes. If Web filters are in place, their access is not equal because they must ask for permission to have the filters disabled. Finally, while most people would agree that children should not be exposed to pornographic material, it would be harder to convince reasonable people that social living would no longer be possible if children happened to see pornography in a library.

Our analysis from the point of view of social contract theory has produced arguments both supporting and opposing the Children's Internet Protection Act. However, installing filters does not seem to be necessary to preserve the public order. For this reason, the issue is outside the social contract and freedom of conscience should be given precedence.

3.6.4 Sexting

Sexting refers to sending sexually suggestive text messages or emails containing nude or nearly nude photographs [65]. In a 2009 survey of 655 American teenagers conducted by Cox Communications, 9 percent said they had sent a sext at least once, 17 percent

said they had received a sext at least once, and 3 percent said they had forwarded a sext at least once. Of the teens who had sent sexts, 11 percent admitted to having sent a sext to someone they didn't know. Interestingly, when those who had sent sexts were asked if a photo they had sent was ever forwarded to someone they didn't want to see it, only 2 percent said "yes," but when the same group of people was asked if their friends ever had photos forwarded to people they didn't want to see it, 30 percent answered "yes" [65].

Although sexting is a relatively recent phenomenon, there are already plenty of stories in the mainstream media about the serious impact it is having on people's lives. Here are three recent stories.

Ohio high school student Jesse Logan sent nude pictures of herself to her boyfriend. When they broke up, the ex-boyfriend distributed the photos to other girls in her high school. Jesse endured months of harassment from her high school classmates and began skipping classes on a daily basis. After attending the funeral of another classmate who committed suicide, Jesse went home and hanged herself [66].

After Phillip Alpert got into an argument with his 16-year-old girlfriend, he emailed a nude photo of her to dozens of her friends and family members. "It was a stupid thing I did because I was upset and tired and it was the middle of the night and I was an immature kid," Alpert said upon reflection. The Orlando, Florida, police arrested Alpert, who had just turned 18, charging him with sending child pornography, a felony. It didn't matter that Alpert's girlfriend was 16, that they had dated for two-and-a-half years, and that she was the one who had originally sent the photo to him. Alpert was sentenced to five years probation and required to register with the state of Florida as a sex offender. He will remain a registered sex offender until he is 43 years old [67].

Ting-Yi Oei, a 59-year-old assistant principal at Freedom High School in South Riding, Virgina, was asked to investigate rumors that students were distributing nude photographs on their cell phones. His investigation led to a 16-year-old boy, who admitted to having a provocative photo on his cell phone. The photo showed the torso of a 17-year-old girl wearing panties, with her arms mostly covering her breasts. Oei showed the image to the principal, who told him to keep a copy on his computer as evidence. Two weeks later, the same boy got in trouble again, and Oei suspended him for two weeks. When Oei met with the boy's mother, he told her about the earlier photo incident. The boy's mother was upset that Oei hadn't immediately told her about the photo, and she demanded that Oei revoke her son's suspension. When Oei refused, the mother went to the police and told them about the photo. Sheriff's investigators came to the school and found the photo of the girl on Oei's computer. County prosecutor James Plowman gave Oei an ultimatum: resign or face felony charges for possession of child pornography. Plowman's assistant told the press, "We just feel very strongly that this is not someone who should be in the Loudoun County school system." Oei refused to resign, and in August 2008, a grand jury indicted him for possession of child pornography. The school district removed him from his position as vice principal and reassigned him to a job at a testing center. Oei had to take out a second mortgage on his house to pay legal expenses. In April 2009, Loudoun Circuit Court Judge Thomas Horne dismissed the charges, noting that nudity alone is not sufficient to categorize an image of a minor as child pornography. Though never convicted, Oei ended up deeply in debt and with a

tarnished reputation, unsure if he would ever return to his former position at the high school [68].

There appears to be a widespread sentiment that child pornography laws should not be used to prosecute teenagers who are caught sexting. In 2009, legislation was introduced in a number of state legislatures that would make sexting among teenagers a misdemeanor [69].

3.7 Breaking Trust on the Internet

3.7.1 Identity Theft

Dorothy Denning defines identity theft as "the misuse of another person's identity, such as name, Social Security number, driver's license, credit card numbers, and bank account numbers. The objective is to take actions permitted to the owner of the identity, such as withdraw funds, transfer money, charge purchases, get access to information, or issue documents and letters under the victim's identity" [70].

The leading form of identity theft in United States is credit card fraud. Identity thieves either take out a new credit card in someone else's name or commandeer an existing account [71]. By changing the billing address of existing accounts, a thief can run up large debts before the victim becomes aware of the problem. These activities can blemish the target's credit history. As a result, victims of identity theft may have applications for credit cards, mortgage loans, and even employment denied. If the impostor shows false credentials to the police, the victim may even be saddled with a false criminal record or outstanding arrest warrants.

Financial institutions contribute to the problem of identity theft by making it easy for people to open up new accounts. Since information brokers on the Web are selling driver's license numbers, Social Security numbers, and credit card information, it's easy for an identity thief to gather a great deal of information about another person. Assuming another person's identity is made simpler by banks allowing people to open accounts online [72].

The number of Americans victimized by identity theft decreased from about 11 million in 2009 to 8 million in 2010, but the average loss increased from $387 to $631 [73]. Fortunately, United States law says that a consumer's liability for losses due to credit card fraud are limited to $50 if reported promptly. Most victims end up paying nothing out-of-pocket because their banks and credit card companies offer zero-liability fraud protection [73]. However, victims of identity theft typically spend more than 30 hours resolving the problem [73].

Most cases of identity theft are not the result of someone using computers to break into a database containing information about a target. Instead, identity thieves are much more likely to use low-tech methods to gain access to the personal information they need. A 2008 survey of identity theft victims revealed that in 43 percent of the cases, the theft was the result of a lost or stolen wallet, credit card, checkbook, or another physical document [74]. Some identity thieves engage in dumpster diving—looking for personal information in garbage cans or recycling bins. Old bills, bank statements, and credit card

statements contain a wealth of personal information, including names, addresses, and account numbers. Another simple way to get information is through shoulder surfing—looking over the shoulders of people filling out forms.

In 19 percent of the cases surveyed in 2008, someone at a business obtained a credit card number when the owner was making a purchase [74]. Waiters or store clerks match each legal swipe through a cash register with an illegal swipe through a skimmer, a small, battery-powered credit card reader. Identity theft rings use numbers collected this way to manufacture counterfeit credit cards.

Surprisingly, 14 percent of the cases of identity theft identified in 2010 were "friendly thefts" in which family members, friends, or in-house employees made purchases without the account-holder's consent [73].

Still, a significant number of people are victims of identity theft through their online activities. Gathering financial information via spam is called phishing (pronounced "fishing"). Thieves send out spam messages designed to look like they originated from PayPal, eBay, or another well-known Internet-active business. Through these messages they hope to con unsuspecting recipients into connecting with authentic-looking Web sites and revealing their credit card numbers or other personal information.

For example, a victim might receive an email message purportedly from PayPal, asking the person to go to the PayPal Web site to confirm a transaction. The email message contains a hypertext link. When the victim clicks on the link, he is connected to the counterfeit PayPal site. Phishing, spyware, and other online methods resulted in more than a million cases of identity theft in the United States in 2008 [74].

The stereotypical victim of identity theft is an elderly person who isn't computer savvy, but the facts speak otherwise. The average age of a victim of identity theft is 40. Many victims are experienced computer users who have become comfortable typing in their credit card information while online [75].

The Identity Theft and Assumption Act of 1998 makes identity theft a federal crime. In 2004, Congress passed the Identity Theft Penalty Enhancement Act, which lengthened prison sentences for identity thieves [76]. A variety of law enforcement agencies investigate alleged violations of this law: the U.S. Secret Service, the FBI, the U.S. Postal Inspection Service, and the Office of the Inspector General of the Social Security Administration [77]. Unfortunately, the probability that a particular case of identity theft will result in an arrest is about 1 in 700 [78].

3.7.2 Chat-Room Predators

Instant messaging is a real-time communication between two or more people supported by computers and a telecommunications system. A chat room is similar to instant messaging, except that it supports discussions among many people. A large number of organizations sponsor chat rooms dedicated to a wide variety of topics. For example, in July 2009, America Online's "Chats" page listed hundreds of chat rooms divided into 30 general categories, including Arts and Entertainment, Black Voices, Friends & Flirts, GLBT, Latino, Life, Places, Politics, Romance, and Town Square.

The popularity of instant messaging varies from country to country. According to Nielsen/NetRatings, the number of people who used instant messaging between January 2002 and March 2002 varied from 13 percent of all Internet users in Denmark to 43 percent in Spain [79]. Participation in chat rooms also varies from country to country. According to the same survey, the number of people with Internet accounts who participated in a chat room between January and March 2002 varied from 16 percent in the United Kingdom to 41 percent in Brazil. Conservatively estimating average use of instant messaging or chat rooms at 25 percent, the number of people worldwide who use this technology at least occasionally is about 150 million.

In 1995, Katie Tarbox, a 13-year-old swimmer from New Canaan, Connecticut, met a man in an AOL chat room [80]. He said his name was Mark and his age was 23. His grammar and vocabulary were good, and he made her feel special. Katie agreed to meet Mark at a hotel in Texas, where her swim team was competing. Soon after she entered his hotel room, he molested her. "Mark" turned out to be 41-year-old Francis Kufrovich from Calabasas, California, a man with a history of preying on children. In March 1998, Kufrovich was the first person in the United States to be sentenced for Internet pedophilia. After pleading guilty, he served 18 months in prison.

In 1999, the FBI investigated 1,500 crimes in which an alleged pedophile crossed a state line to meet and molest a child met through an Internet chat room [80]. Many say the problem is growing. Parry Aftab, executive director of Cyber Angels, says, "I know that I can go into a chat room as a 12-year-old and not say anything, and be hit on and asked if I'm a virgin within two minutes" [80]. In New York a 42-year-old man was sentenced to 150 years in prison after being convicted of kidnapping a 15-year-old girl and raping her repeatedly over the course of a week. He met the girl in a chat room [81].

Police have begun entering chat rooms posing as young girls to lure pedophiles [82]. During a three-week-long sting operation in Spokane, Washington, a police detective posed as a 13-year-old girl in a chat room. In early March 2003, police arrested a 22-year-old man on charges of attempted second-degree rape of a child. Inside his car the officers found handcuffs, a large folding knife, and a condom. The suspect was still on parole for an earlier conviction for fourth-degree assault with sexual motivation. Police sergeant Joe Petersen asked, "What happens had it been a real girl?" [81]. Chat-room sting operations are leading to many arrests all over the United States [83, 84, 85, 86, 87, 88].

3.7.3 Ethical Evaluations of Police "Sting" Operations

Is it morally right for police detectives to entrap pedophiles by posing as children in chat rooms and agreeing to meet with them?

UTILITARIAN ANALYSIS

Let's consider the various consequences of such a sting operation. A person allegedly interested in having sex with an underage minor is arrested and charged with attempted child rape. Suppose the person is found guilty and must serve time in prison. The direct effects of the sting operation are the denial of one person's freedom (a harm) and an

increase in public safety (a benefit). Since the entire public is safer and only a single person is harmed, this is a net good.

The sting operation also has indirect effects. Publicity about the sting operation may deter other chat-room pedophiles. This, too, is a beneficial result. It is harder to gauge how knowledge of sting operations influences innocent citizens. First, it may reduce citizens' trust in the police. Many people believe that if they are doing nothing wrong, they have nothing to fear. Others may become less inclined to provide information to the police when requested. Second, sting operations can affect everyone's chat-room experiences. They demonstrate that people are not always who they claim to be. This knowledge may make people less vulnerable to being taken advantage of, but it may also reduce the amount of trust people have in others. Sting operations prove that supposedly private chat-room conversations can actually be made public. If chat-room conversations lack honesty and privacy, people will be less willing to engage in serious conversations. As a result, chat rooms lose some of their utility as communication devices. How much weight you give to the various consequences of police sting operations in chat rooms determines whether the net consequences are positive or negative.

KANTIAN ANALYSIS

A Kantian focuses on the will leading to the action rather than the results of the action. The police are responsible for maintaining public safety. Pedophiles endanger innocent children. Therefore, it is the duty of police to try to prevent pedophiles from accomplishing what they intend to do. The will of the police detective is to put a pedophile in prison. This seems straightforward enough.

If we dig a level deeper, however, we run into trouble. In order to put a pedophile in prison, the police must identify this person. Since a pedophile is unlikely to confess on the spot if asked a question by a police officer, the police lay a trap. In other words, the will of the police detective is to deceive a pedophile in order to catch him. To a Kantian, lying is wrong, no matter how noble the objective. By collecting evidence of chat-room conversations, the police detective also violates the presumed privacy of chat rooms. These actions of the police detective affect not only the alleged pedophile, but also every innocent person in the chat room. In other words, detectives are using every chat-room occupant as a means to their end of identifying and arresting the pedophile. While police officers have a duty to protect the public safety, it is wrong for them to break other moral laws in order to accomplish this purpose. From a Kantian point of view, the sting operation is morally wrong.

SOCIAL CONTRACT THEORY ANALYSIS

An adherent of social contract theory could argue that in order to benefit everyone, there are certain moral rules that people in chat rooms ought to follow. For example, people ought to be honest, and conversations ought to be kept confidential. By misrepresenting identity and/or intentions, the pedophile has broken a moral rule and ought to be punished. In conducting sting operations, however, police detectives also misrepresent their identities and record everything typed by suspected pedophiles. The upholders of the law have broken the rules, too. Furthermore, we have the presumption of innocence

until proof of guilt. What if the police detective, through miscommunication or bad judgment, actually entraps someone who is not a pedophile? In this case, the innocent chat-room users have not broken any rules. They were simply in the wrong place at the wrong time. Yet society, represented by the police detective, did not provide the benefits chat-room users expect to receive (honest communications and privacy). In short, there is a conflict between society's need to punish a wrongdoer and its expectation that everyone (including the agents of the government) will abide by its moral rules.

SUMMARY OF ETHICAL ANALYSES

To summarize our ethical evaluation of police sting operations, the actions of the police seem immoral from a Kantian point of view. Evaluations using the other ethical theories do not yield a clear-cut endorsement or condemnation of the stings. While the goals of the police are laudable, they accomplish their goals by deceiving other chat-room users and revealing details of conversations thought to be private. Sting operations are more likely to be viewed as morally acceptable by someone who is more focused on the results of an action than the methods used; in other words, a consequentialist.

3.7.4 False Information

The Web is a more open communication medium than newspapers, radio stations, or television stations. Individuals or groups whose points of view may never be published in a newspaper or broadcast on a television or radio show may create an attractive Web site. The ease with which people may get information out via the Web is one of the reasons the Web contains billions of pages. However, the fact that no one has to review a Web page before it is published means the quality of information available on the Web varies widely.

You can find many Web sites devoted to the American manned space program. You can also find many Web sites that provide evidence the moon landings were a hoax by NASA. Many Web sites describe the Holocaust committed by the Nazis before and during World War II. Other sites explain why the Holocaust could not have happened.

Disputes about commonly held assumptions did not begin with the Web. Some television networks and newspapers are well known for giving a forum to people who question information provided through government agencies. Twice in 2001, the Fox TV network aired a program called "Conspiracy Theory: Did We Land on the Moon?" The program concludes NASA faked the moon landing in the Nevada desert. Supermarket tabloids are notorious for their provocative, misleading headlines. Experienced consumers take into account the source of the information. Most people would agree that *60 Minutes* on CBS is a more reliable source of information than *Conspiracy Theory* on Fox. Similarly, people expect information they find in *The New York Times* to be more reliable than the stories they read in a tabloid.

In traditional publishing, various mechanisms are put in place to improve the quality of the final product. For example, before Addison-Wesley published the first edition of this book, an editor sent draft copies of the manuscript to a dozen reviewers who checked it for errors, omissions, or misleading statements. The author revised the man-

uscript to respond to the reviewers' suggestions. After the author submitted a revised manuscript, a copy editor made final changes to improve the readability of the text, and a proofreader corrected typographical errors.

Web pages, on the other hand, can be published without any review. As you're undoubtedly well aware, the quality of Web pages varies dramatically. Fortunately, search engines can help people identify those Web pages that are most relevant and of the highest quality. Let's take a look at how the Google search engine does this.

The Google search engine keeps a database of many billions of Web pages. A software algorithm ranks the quality of these pages. The algorithm invokes a kind of voting mechanism. If Web page A links to Web page B, then page B gets a vote. However, all votes do not have the same weight. If Web page A is itself getting a lot of votes, then page A's link to page B gives its vote more weight than a link to B from an unpopular page.

When a user makes a query to Google, the search engine first finds the pages that closely match the query. It then considers their quality (as measured by the voting algorithm) to determine how to rank the relevant pages.

3.7.5 Cyberbullying

In November 2002, Ghyslain Raza, a chubby high school student living in Quebec, Canada, borrowed a videotape and used one of the high school's video cameras to film himself swinging a golf ball retriever like a light saber, à la Darth Maul in *Star Wars Episode I*. A few months later, the owner of the videotape discovered the content and shared it with some friends. After one of them digitized the scene and made it available on the Internet, millions of people downloaded the file in the first two weeks [90]. Ghyslain was nicknamed "the Star Wars kid," endured prolonged harassment from other students, and eventually dropped out of school [91]. By 2006, the video had been viewed more than 900 million times [92].

Cyberbullying is the use of the Internet or the phone system to inflict psychological harm on another person. Frequently, a group of persons gangs up to cyberbully the victim. Examples of cyberbullying include:

- Repeatedly texting or emailing hurtful messages to another person
- Spreading lies about another person
- Tricking someone into revealing highly personal information
- "Outing" or revealing someone's secrets online
- Posting embarrassing photographs or videos of other people without their consent
- Impersonating someone else online in order to damage that person's reputation
- Threatening or creating significant fear in another person

Surveys have revealed that cyberbullying is common among teenagers. Cox Communications surveyed 655 American teenagers in 2009, and 19 percent reported that they had been cyberbullied online, via cell phone, or through both media. Ten percent

of the teenagers admitted to cyberbullying someone else. When asked why they had cyberbullied someone else, the most common responses were, "They deserved it" and, "To get back at someone" [65].

In some instances cyberbullying has led to the suicide of the victim, as in the case of 13-year-old Megan Meier. According to her mother, "Megan had a lifelong struggle with weight and self-esteem" [93]. She had talked about suicide in third grade, and ever since then she had been seeing a therapist [93]. Megan's spirits soared when she met a 16-year-old boy named Josh Evans on MySpace. They flirted online for four weeks but never met in person. Then Josh seemed to sour on their relationship. One day he let her know that he didn't know if he wanted to be friends with her anymore. The next day he posted [93, 94]:

```
You are a bad person and everybody hates you.
Have a shitty rest of your life.
The world would be a better place without you.
```

When Megan angrily responded to this post, others ganged up on her: "Megan Meier is a slut. Megan Meier is fat." [93]. Later that afternoon, Megan hanged herself in her bedroom.

Eventually, the community learned that "Josh Evans" did not exist. The MySpace account had been created just a couple of houses away from the Meier home by 18-year-old Ashley Grills, 13-year-old Sarah Drew, and Lori Drew, Sarah's mother. Sarah had had a falling out with Megan, and Ashley suggested creating the MySpace account to find out what Megan might be saying about Sarah. Lori Drew had approved the plan. Most of the messages from "Josh" had been written by Sarah or Ashley, but Lori Drew had been aware of what they were doing [95].

The county's district attorney declined to prosecute Lori Drew because there was no Missouri law against cyberbullying [96]. The FBI investigated the case, however, and in 2008, federal prosecutors charged Drew with four felony counts under the Computer Fraud and Abuse Act for violating the MySpace terms of service. A jury found her not guilty of these crimes but did convict her of three misdemeanors [97]. In 2009, a U.S. district judge overturned these convictions, stating that criminal charges should not have been brought against Drew for breaking a contract with an Internet service provider [98].

In April 2009, the Megan Meier Cyberbullying Prevention Act was introduced in the U.S. House of Representatives. The purpose of the proposed law was to "impose criminal penalties on anyone who transmits in interstate or foreign commerce a communication intended to coerce, intimate, harass, or cause substantial emotional distress to another person, using electronic means to support severe, repeated, and hostile behavior" [99]. Some civil libertarians objected to the proposed legislation, arguing that it would take away free speech rights guaranteed under the First Amendment to the U.S. Constitution. The law did not win approval by the House of Representatives.

3.8 Internet Addiction

3.8.1 Is Internet Addiction Real?

Using an Internet-enabled computer can be a lot of fun—the number of different things you can do online is staggering. Some psychologists warn about the dangers of Internet addiction. Are these fears justified?

In 1976, long before most computers were networked, Joseph Weizenbaum pointed out what attracts computer programmers to their machines: feelings of freedom and power. Because programmers deal with bits instead of physical objects, they are largely free to create whatever they can imagine, and computers execute their instructions without hesitation. The resulting thrill causes some programmers to have a "compulsion to program." In Weizenbaum's words:

> [B]right young men of disheveled appearance, often with sunken glowing eyes, can be seen sitting at computer consoles, their arms tensed and waiting to fire their fingers, already poised to strike, at the buttons and keys on which their attention seems to be as riveted as a gambler's on the rolling dice . . . They work until they nearly drop, twenty, thirty hours at a time. Their food, if they arrange it, is brought to them: coffee, Cokes, sandwiches. If possible, they sleep on cots near the computer. But only for a few hours—then back to the console or the printouts. Their rumpled clothes, their unwashed and unshaven faces, and their uncombed hair all testify that they are oblivious to their bodies and to the world in which they move. They exist, at least when so engaged, only through and for the computers [89].

Weizenbaum's observation is echoed by Maressa Orzack, who states, "Computer addiction is real . . . As an impulse control disorder, computer addiction resembles pathological gambling" [100].

The traditional definition of addiction is the persistent, compulsive use of a chemical substance, or drug, despite knowledge of its harmful long-term consequences [101]. Today, however, Orzack and some other psychologists and psychiatrists have extended the definition of addiction to include any persistent, compulsive behavior that the addict recognizes to be harmful. According to their broader definition of addiction, people can be addicted to gambling, food, sex, long-distance running, and other activities, including computer-related activities [102].

Some people spend between 40 and 80 hours per week on the Internet, with individual sessions lasting up to 20 hours [103, 104]. Spending so much time online can have a wide variety of harmful consequences. Fatigue from sleep deprivation can lead to unsatisfactory performance at school or at work. Physical ailments include carpal tunnel syndrome, back strain, and eyestrain. Too many hours in front of a computer can weaken or destroy relationships with friends and family members [103]. In a few cases, people have died after prolonged sessions sitting in front of a computer.

Kimberly Young has created a test for Internet addiction. Using the diagnosis of pathological gambling in the *Diagnostic and Statistical Manual of Mental Disorders* as

her starting point, Young has produced an eight-question screening instrument, which I reproduce verbatim [105]:[1]

1. Do you feel preoccupied with the Internet (think about previous online activity or anticipate next online session)?
2. Do you feel the need to use the Internet with increasing amounts of time in order to achieve satisfaction?
3. Have you repeatedly made unsuccessful efforts to control, cut back, or stop Internet use?
4. Do you feel restless, moody, depressed, or irritable when attempting to cut down or stop Internet use?
5. Do you stay online longer than originally intended?
6. Have you jeopardized or risked the loss of significant relationship, job, educational or career opportunity because of the Internet?
7. Have you lied to family members, therapist, or others to conceal the extent of involvement with the Internet?
8. Do you use the Internet as a way of escaping from problems or of relieving a dysphoric mood (e.g., feelings of helplessness, guilt, anxiety, depression)?

Young considers patients who answer "yes" to five or more of these questions to be addicted to the Internet, unless "their behavior could not be better accounted for by a Manic Episode" [103].

Young's use of the phrase "Internet addiction" and her questionnaire are controversial. John Charlton points out that computer use, unlike drug use, is generally considered to be a positive activity. In addition, while drug addiction leads to an increase in criminal activity, the same level of societal harm is unlikely to occur even if the Internet is overused by some people. Charlton performed his own study of computer users and has concluded that Young's checklist approach is likely to overestimate the number of people addicted to the Internet. According to Charlton, some "people who are classified as computer-dependent or computer-addicted might often be more accurately said to be highly computer-engaged" [106].

Mark Griffiths holds a position similar to Charlton, stating that "to date there is very little empirical evidence that computing activities (i.e., Internet use, hacking, programming) are addictive" [104]. Richard Ries argues that it would be more accurate to call excessive use of the Internet a compulsion [107].

However, others share Young's perspective. Stanton Peele maintains that "people become addicted to experiences" [102]. In his broader view of addiction, non-drug experiences can be addictive. Peele has developed a model of addiction that extends "to all areas of repetitive, compulsive behavior" [102].

1. "Internet Addiction: The Emergence of a New Clinical Disorder," by Kimberly S. Young from CYBERPSYCHOLOGY AND BEHAVIOR. Copyright © 1998 by Mary Ann Liebert, Inc. Publishers. Reprinted with permission.

Our concern in this section is excessive Internet use that causes harm. The dispute over terminology is not important to our discussion. We will use the term "Internet addiction" rather than "Internet compulsion," since the former term appears to be more widely used by the press.

3.8.2 Contributing Factors

According to Peele, social, situational, and individual factors can increase a person's susceptibility to addiction. For example, peer groups play an important role in determining how individuals use alcohol and other drugs. People in stressful situations are more likely to become addicted, as are those who lack social support and intimacy, and those who have limited opportunities for "rewarding, productive activity" [102]. Individual factors that make a person more susceptible to addiction include a tendency to pursue an activity to excess, a lack of achievement, a fear of failure, and feelings of alienation.

Young's studies have led her to "believe that behaviors related to the Internet have the same ability to provide emotional relief, mental escape, and ways to avoid problems as do alcohol, drugs, food, or gambling" [103]. She notes that the typical Internet addict is addicted to a single application.

3.8.3 Ethical Evaluation of Internet Addiction

People who use the Internet excessively can harm themselves and others for whom they are responsible. For this reason, excessive Internet use is a moral issue.

Kantianism, utilitarianism, and social contract theory all share the Enlightenment view that individuals, as rational beings, have the capacity and the obligation to use their critical judgment to govern their lives [108]. Kant held that addiction is a vice, because it's wrong to allow your bodily desires to dominate your mind [109]. Mill maintained that some pleasures are more valuable than others and that people have the obligation to help each other "distinguish the better from the worse" [50].

Ultimately, people are responsible for the choices they make. Even if an addict is "hooked," the addict is responsible for choosing to engage in the activity the first time. This view assumes that people are capable of controlling their compulsions. According to Jeffrey Reiman, vices are "dispositions that undermine the sovereignty of practical reason. Dispositions, like habits, are hard but not impossible to overcome, and undermining something weakens it without necessarily destroying it entirely" [108].

Reiman's view is supported by Peele, who believes addicts can choose to recover from their addictions. "People recover to the extent that they (1) believe an addiction is hurting them and wish to overcome it, (2) feel enough efficacy to manage their withdrawal and life without the addiction, and (3) find sufficient alternative rewards to make life without the addiction worthwhile" [102].

While our analysis to this point has concluded that individual addicts are morally responsible for their addictions, it's also possible for a society to bear collective moral responsibility for the addictions of some of its members. We have already discussed how

social conditions can increase a person's susceptibility to addiction, and Peele states an addict will not recover unless life without the addiction has sufficient rewards.

Addiction is wrong because it means voluntarily surrendering the sovereignty of your reason by engaging in a compulsion that has short-term benefits but harms the quality of your life in the long term. However, if somebody is living in a hopeless situation where any reasonable person would conclude there are no long-term prospects for a good life, then what is lost by giving in to the compulsion? Reiman believes that this is the case for many American inner-city drug addicts. "They face awful circumstances that are unjust, unnecessary, and remediable, and yet that the society refuses to remedy. Addiction is for such individuals a bad course of action made tolerable by comparison to the intolerable conditions they face. In that face, I think that moral responsibility for their strong addictions . . . passes to the larger society" [108].

Of course, the circumstances facing a typical suburban Internet addict are radically different from those facing a typical inner-city drug addict. For this reason, it is tempting to dismiss the notion that society could in any way be responsible for the Internet addiction of some of its members. However, some people use the Internet as a way to escape into their own world, because in the "real world" they suffer from social isolation [104]. Perhaps we should reflect on whether any of our actions or inactions make certain members of our community feel excluded.

Summary

The Internet and the telephone system are powerful and flexible tools that support a wide variety of social interactions. In this chapter, we have explored text messaging, email, chat rooms, and the Web. All of these technologies have had both positive and negative impacts on society.

Twenty years ago, relatively few people had email accounts. Back then, email advertising was virtually unheard of. Email users did not have to delete large numbers of unwanted messages from their mailboxes. On the other hand, email was not too useful outside work, because most people didn't have it.

Today, well over a billion people have an email account. Most anyone you'd like to communicate with has an email address. However, the large number of email users has attracted the attention of direct marketing firms. In the past few years the volume of unsolicited bulk email (spam) has risen dramatically. Many believe the presence of spam has harmed the email system, and a variety of steps have been taken to filter out spam messages before they reach users.

The Web contains over one trillion pages. It contains images of sublime beauty and shocking cruelty, uplifting poetry and expletive-ridden hate speech, well-organized encyclopedias and figments of paranoid imaginations. In short, it is a reflection of the best and the worst of humanity. Web-based social networking sites such as Facebook and Twitter have attracted hundreds of millions of users and created new communication paradigms. Some point to the use of Facebook and Twitter by participants in the Arab

Spring uprising as evidence that these tools can be powerful agents for social change, while others think the impact of these tools has been overblown.

Governments have responded to the idea-sharing potential of the Web and social networking sites in a variety of ways. The most repressive governments have simply made the Internet inaccessible to their people. Other governments have instituted controls that prevent certain sites from being accessed. Most governments allow their citizens nearly universal access to Web sites and Web-based applications.

In the United States, there have been numerous efforts to make pornography inaccessible to children via the Web. The U.S. Congress passed three laws attempting to make pornography less accessible to children via the Web. All of these laws raised objections from civil libertarians, who called them an infringement on free speech rights. The U.S. Supreme Court ruled the first two laws unconstitutional; it upheld the third.

Given the amount of legislation that has been passed to protect children from pornography, it is ironic that many teenagers have become a source of suggestive images. The legal system has not yet caught up with sexting: the use of email or cell phones to send messages containing photos of nude or partially nude people. Child pornography laws were written with pedophiles in mind. What is the proper response to minors who are sexting photos of themselves?

The Internet provides new ways for people to be misled. For example, chat rooms are a popular way for groups of like-minded people to come together to discuss a topic of mutual interest. Unfortunately, sexual predators have used chat rooms as a tool to contact children. In response, police have begun to set up "sting" operations to snare these predators. While sting operations may catch sexual predators, they also change the climate of chat rooms.

The Internet has facilitated e-commerce. Many people are comfortable purchasing items over the Internet. Submitting a credit card number and other identifying information is part of this process. In this environment, the problem of identity theft is a serious concern. Every year, millions of people are conned into revealing their credit card numbers to scam artists who use this information to get cash advances or purchase goods using someone else's identity.

The Web provides a remarkably simple way for people to post and access information. People looking for answers can often get more information, and get it much more quickly, by retrieving what they want from the Web instead of searching printed encyclopedias, books, journals, and newspapers. Ordinary people can also use the Web to broadcast their ideas around the globe. There are many advantages to this information-rich environment. Unfortunately, because anybody can post information on the Web, incorrect information is mixed in with correct information. Web users cannot believe everything they read on the Web. Web search engines incorporate algorithms that attempt to steer people toward higher-quality sites.

The Internet and the telephone system have provided a new way for people to intimidate or humiliate others. After Megan Meier was cyberbullied, she took her own life. The adult involved in the cyberbullying was not prosecuted by local authorities because there were no state laws against cyberbullying. Efforts to create a national cyberbullying

law in the United States drew objections from civil libertarians, who feared that it would greatly restrict freedom of expression, and the law was not passed.

A wide variety of enticing activities are available online, and some people exhibit a compulsion to spend extraordinarily long hours connected to the Internet. Numerous commentators have compared compulsive computer users to compulsive gamblers. Whether or not a compulsive online activity is a true addiction, excessive computer use can have harmful consequences. According to Kantianism, utilitarianism, and social contract theory, people must take responsibility for the voluntary choices they make, including the decision to go online. However, we should also remember that social and cultural factors can make people more susceptible to addictions.

Review Questions

1. What is the Internet?
2. Explain the meaning of the two parts of an email address.
3. Describe how email is transmitted from the sender to the recipient.
4. What is spam?
5. What does a spam filter do?
6. What is a URL?
7. What is a wiki?
8. What is a blog?
9. What is a PC bang?
10. Describe five uses of the Web not covered in the text.
11. Define censorship in your own words.
12. Summarize the different forms of direct censorship.
13. According to the U.S. Supreme Court, why do broadcasters have the most limited First Amendment rights?
14. What characteristics of the Internet make censorship difficult?
15. What is a Web filter?
16. What is sexting?
17. What is the leading form of identity theft in the United States?
18. What is phishing?
19. Define cyberbullying in your own words.
20. How does the idea of "Internet addiction" stretch the traditional concept of addiction?
21. What is the Enlightenment view regarding responsibility for addiction?

Discussion Questions

22. Why is texting more popular than making phone calls?
23. Should nonprofit organizations be regulated the same way as for-profit organizations with respect to their use of unsolicited bulk email?
24. Why is "cold calling" considered to be an acceptable sales practice, but spamming isn't?
25. Suppose a fee (an electronic version of a postage stamp) was required in order to send an email message. How would this change the behavior of email users? Suppose the fee was one cent. Do you think this would solve the problem of spam?
26. Internet service providers monitor their chat rooms and expel users who violate their codes of conduct. For example, users can be kicked off for insulting a person or a group of people based on their race, religion, or sexual orientation. Is it wrong for an ISP to expel someone for hate speech?
27. Suppose you are the director of an ISP that serves the email needs of 10,000 customers. You receive dozens of complaints from them every week about the amount of spam they are receiving. Meanwhile, American spammers are hacking into computers in Jamborea (an East Asian country) and using them to mail spam back to the United States. You estimate that at least 99 percent of email originating from Jamborea is spam. A few of the messages, however, are probably legitimate emails. Should you do anything to restrict the flow of email messages from Jamborea to your customers?
28. Stockbrokers are now required to save all their instant messaging communications. Is having a record of everything you type good or bad? Do you think this requirement will change the behavior of brokers?
29. There is a thriving "real world" market for gold, artifacts, and avatars from virtual worlds such as *World of Warcraft*. In effect, rich Westerners are offshoring game-playing to China. Do you find this image disturbing?
30. What are the benefits and harms of Internet censorship?
31. Should citizens of democratic nations help people in authoritarian nations get around the Web censorship of their repressive governments?
32. Should people publishing accusations against others on their blogs or MySpace pages be held responsible if they disseminate false information?
33. Should a college or university have the right to suspend its students who brag about breaking its rules on their Facebook or MySpace pages?
34. Discuss similarities and differences between the Web and each of these other ways that we communicate: the telephone system, physical mail, bookstores, movie theaters, newspapers, broadcast and cable TV. Should governments ignore the Web, or should they regulate it somehow? If governments should regulate the Web, should the regulations be similar to the regulations for one of the aforementioned communication systems, or should they be unique in significant ways?
35. The convenience of Wikipedia makes it a popular reference for students. After several instances in which students cited incorrect information, however, the history department at Middlebury College prohibited references to Wikipedia articles in papers or exams.

Did the Middlebury history department go too far? What is the proper role, if any, for Wikipedia in academic research?

36. Should bloggers be given the same rights as newspaper, magazine, or television journalists?

37. Should children be prevented from accessing some Web sites? Who should be responsible for the actions of children surfing the Web?

38. A female employee of a high-tech company receives on average 40 spam messages per day. About one-quarter of them are advertising pornographic Web sites and have photographs of naked women. All of these emails pass through the company's email server. The woman sues the company for sexual harassment, saying that the company tolerates an atmosphere that is degrading to women. Is the company responsible for the pornographic spam reaching the computers of its employees?

39. You are in charge of the computers at a large, inner-city library. Most of the people who live in the neighborhood do not have a computer at home. They go to the library when they want to access the Internet. About two-thirds of the people surfing the Web on the library's computers are adults.

    You have been requested to install filtering software that would block Web sites containing various kinds of material deemed inappropriate for children. You have observed this software in action and know that it also blocks many sites that adults might legitimately want to visit. How should you respond to the request to install filtering software?

40. Are there any circumstances under which sexting is morally acceptable?

41. What is the age at which a parent or guardian should provide a child with a cell phone? Should younger children be provided with cell phones having fewer features?

42. Discuss the morality of Google's page-ranking algorithm. Does it systematically exclude Web pages containing opinions held only by a small segment of the population? Should every opinion on the Web be given equal consideration?

43. What is the longest amount of time you have ever spent in a single session in front of a computer? What were you doing?

44. The income of companies providing persistent online games depends on the number of subscribers they attract. Since consumers have a choice of many products, each company is motivated to create the best possible experience for its customers. Role-playing adventures have no set length. When playing one of these games, it's easy to spend more time on the computer than originally planned. Some subscribers cause harm to themselves and others by spending too much time playing these games. Should the designers of persistent online games bear some moral responsibility for this problem?

45. A school district forbids students from using their cell phones on school buses, but many students ignore this rule. A frustrated bus driver installs a cell phone jammer on his bus. When the jammer is turned on, cell phones within 40 feet stop working. (The use of jammers is against the law.) The bus driver says, "The kids think they are sneaky by hiding low in their seats and using their phones. Now the kids can't figure out why their phones don't work, but can't ask because they will get in trouble! It's fun to watch them try to get a signal" [110].

    Discuss the morality of the bus driver's use of the jammer.

46. According to some commentators, Facebook and Twitter played a vital role in the Arab Spring uprising because they made it possible for activists to organize large protests in a short amount of time. Others argue that Facebook and Twitter were simply tools used by activists and that genuine social grievances led to the revolutions in Tunisia and Egypt. What is your view?

47. After popular uprisings in Tunisia and Egypt in 2011, the United States government said it would spend $30 million to fund the development of new services and technologies designed to allow activists in other countries to get around Internet restrictions imposed by their governments.

    Announcing this initiative, Secretary of State Hillary Clinton said, "We are convinced that an open Internet fosters long-term peace, progress and prosperity. The reverse is also true. An Internet that is closed and fractured, where different governments can block activity or change the rules on a whim—where speech is censored or punished, and privacy does not exist—that is an Internet that can cut off opportunities for peace and progress and discourage innovation and entrepreneurship" [111].

    Should the U.S. government provide activists in other countries the tools to get around Internet restrictions imposed by authoritarian governments?

48. In July 2011, activists shut down a San Francisco subway station as a way of protesting the death of a drunk man shot by a Bay Area Rapid Transit (BART) police officer [112]. A month later, the subway system blocked cell phone service at several stations in an effort to prevent another protest. According to BART officials, protesters had said they "would use mobile devices to coordinate their disruptive activities and communicate about the location and number of BART Police" [113]. The agency said, "A civil disturbance during commute times at busy downtown San Francisco stations could lead to platform overcrowding and unsafe conditions for BART customers, employees and demonstrators" [113].

    Was BART justified in blocking cell phone service?

In-Class Exercises

49. Divide the class into groups. Each group should come up with a variant of the case study "Ann the Acme Accountant," in which both a Kantian evaluation and an act utilitarian evaluation would conclude Ann did something wrong.

50. Divide the class into groups. Each group should come up with a variant of the case study "Kate's Blog," in which the analysis from the perspective of social contract theory would conclude Kate did nothing wrong, but an act utilitarian evaluation would conclude Kate did something wrong.

51. Divide the class into teams representing each of the following groups:

    - Small, struggling business
    - Large, established corporation
    - Internet service provider
    - Consumer

    Discuss the value of direct email versus other forms of advertising, such as direct mail, television advertising, radio advertising, the Yellow Pages, and setting up a Web site.

52. A company uses pop-up advertising to market its software product, which blocks pop-ups from appearing when someone is surfing the Web. Debate the morality of the company's marketing strategy.

53. Ad-blocking software attachments to Web browsers enable a Web surfer to visit Web sites without having to view the pop-up advertisements associated with these Web pages. Debate this proposition: "People who use ad-blocking software are violating an implicit 'social contract' with companies that use advertising revenues as a means of providing free access to Web pages."

54. In 2000, the Estonian parliament passed a law declaring Internet access to be a fundamental human right of its citizens. Divide the class into two groups (pro and con) to debate the following proposition: Internet access should be a fundamental human right, along with the such other fundamental human rights as the right to life and the right to free speech.

55. How do you determine the credibility of information you get from the Web? Does the source of the information make any difference to you? If so, how would you rank the reliability of each of the following sources of Web pages? Does the type of information you're seeking affect your ranking?
    - Establishment newspaper
    - Counterculture newspaper
    - Television network
    - Corporation
    - Nonprofit organization
    - Individual

56. Martin Dula has suggested that parents should not provide their children with phones capable of taking photos and videos because these phones tempt children to participate in sexting [67].

    Debate the following proposition: Parents and legal guardians should not allow their children under the age of 18 to own cell phones capable of taking, transmitting, or receiving photographs or videos.

Further Reading

Chris Anderson and Michael Wolff. "The Web Is Dead. Long Live the Internet." *Wired*, September 2010. www.wired.com.

Anand Giridharadas. "Where a Cellphone Is Still Cutting Edge." *The New York Times*, April 9, 2010. www.nytimes.com.

Malcolm Gladwell. "Small Change: Why the Revolution Will Not Be Tweeted." *The New Yorker*, October 4, 2010.

Aldous Huxley. *Brave New World*. Harper Perennial Modern Classics, 2006. (Originally published in 1932.)

Steven Levy. "How Early Twitter Decisions Led to Anthony Weiner's Dickish Demise." *Wired Epicenter*, June 13, 2011. www.wired.com/epicenter/.

Steven Levy. "Mob Rule! How Users Took Over Twitter." *Wired*, November 2009. www.wired.com.

Gary Wolf. "The Tragedy of Craigslist." *Wired*, September 2009. www.wired.com.

Allen Salkin. "Party On, But No Tweets." *The New York Times*, August 9, 2009. www.nytimes.com.

Cass R. Sunstein. *Democracy and the Problem of Free Speech*. The Free Press, New York, NY, 1993.

Brian Whitworth and Elizabeth Whitworth. "Spam and the Social-Technical Gap." *Computer* 37(10):38–45, October 2004.

References

[1] Alex Williams. "Mind Your BlackBerry or Mind Your Manners," *The New York Times*, June 22, 2009. www.nytimes.com.

[2] Neda Ulaby. "The Posies: How Do Bands Make Money Now?" *National Public Radio: All Things Considered (radio show)*, July 29, 2009. www.npr.org.

[3] "Internet Overtakes Newspapers as News Outlet." Pew Research Center for the People & the Press, December 23, 2008. pewresearch.org.

[4] Jose Antonio Vargas. "Obama Raised Half a Billion Online." *WashingtonPost.com*, November 20, 2008.

[5] "Paul Sets One-day GOP Fundraising Record." *MSNBC*, November 6, 2007. www.msnbc.msn.com.

[6] "The Radicati Group, Inc. Releases Q2 2008 Market Numbers Update," June 18, 2009. www.radicati.com.

[7] Brad Templeton. "Origin of the Term 'Spam' to Mean Net Abuse," July 8, 2005. www.templetons.com/brad/spamterm.html.

[8] Peter H. Lewis. "An Ad (Gasp!) in Cyberspace." *The New York Times*, April 19, 1994.

[9] "Filters Getting Better at Blocking Spam." *The Boston Globe*, May 12, 2009.

[10] Saul Hansell. "Internet Is Losing Ground in Battle against Spam." *The New York Times*, April 22, 2003.

[11] Joe Stewart. "Top Spam Botnets Exposed." April 8, 2008. www.secureworks.com/research/threats/topbotnets.

[12] Brian Whitworth and Elizabeth Whitworth. "Spam and the Social-Technical Gap." *Computer* 37(10):38–45, October 2004.

[13] Tim Berners-Lee. *Weaving the Web*. HarperCollins Publishers, New York, NY, 1999.

[14] Erick Schonfeld. "Forrester Forecast: Online Retail Sales Will Grow to $250 Billion by 2014." *Tech Crunch*, March 8, 2010. techcrunch.com.

[15] Daniel H. Pink. "The Book Stops Here." *Wired*, page 125, March 2005.

[16] Paul Festa. "Dialing for Bloggers." *The New York Times*, February 25, 2003.

[17] Rebecca Kern. "Free Online Course Offerings Grow in Abundance and Popularity." *U.S. News and World Report*, February 12, 2010. www.usnews.com.

[18] Associated Press. "50 Million Historical Documents Posted on Web." *CNN.com*, April 5, 2003.

[19] "World of Warcraft Reaches New Milestone: 10 Million Subscribers." Blizzard Entertainment, January 22, 2008. eu.blizzard.com.

[20] Tim Ingham. "CHINA: Warcraft Hits One Million Unique Users." *MCV*, April 14, 2008. www.mcvuk.com.

[21] Jimmy Yap. "Power Up!" *Internet Magazine*, February 2003.

[22] David Barboza. "Ogre to Slay? Outsource It to China." *The New York Times*, December 9, 2005.

[23] Associated Press. "IRS Online Filing Tops 2M Users." *The New York Times*, March 25, 2003.

[24] "Internet Gambling Yield Passes US$20bn: Online Gambling Shows Resilience in Face of Recession." *Reuters*, March 9, 2009. www.reuters.com.

[25] Bob Tedeschi. "Gambling Sites Adjust to Scrutiny." *The New York Times*, March 31, 2003.

[26] www.kiva.org.

[27] Maggie Shiels. "Twitter Co-founder Jack Dorsey Rejoins Company." *BBC News*, March 28, 2011. www.bbc.co.uk.

[28] Emma Barnett. "Twitter Record Broken During the Women's World Cup Final." *The Telegraph* (London, England). www.telegraph.co.uk.

[29] Claire Cain Miller. "Mom-and-Pop Operators Turn to Social Media." *The New York Times*, July 23, 2009.

[30] Philip N. Howard. "The Arab Spring's Cascading Effects." *Miller-McCune*. www.miller-mccune.com.

[31] "Region in Turmoil." *Al Jazeera*. Accessed August 8, 2011. blogs.aljazeera.net/twitter-dashboard.

[32] William Saletan. "Springtime for Twitter." *Slate*, July 18, 2011. www.slate.com.

[33] Malcolm Gladwell. "Small Change: Why the Revolution Will Not Be Tweeted." *The New Yorker*, October 4, 2011.

[34] "About Filtering." August 1, 2007. opennet.net/about-filtering.

[35] Privacy International. "Silenced—Burma." September 21, 2003. www.privacyinternational.org.

[36] Stephen Gibbs. "Cuba Law Tightens Internet Access." *BBC News*, January 24, 2004.

[37] Rebecca MacKinnon. "Chinese Cell Phone Breaches North Korean Hermit Kingdom." *YaleGlobal Online*, January 17, 2005.

[38] Jonathan Zittrain and Benjamin Edelman. "Documentation of Internet Filtering in Saudi Arabia." Technical report, Harvard Law School, Cambridge, MA, September 12, 2002.

[39] Rebekah Heacock. "China Shuts Down Internet in Xinjiang Region after Riots." *OpenNet Initiative*, July 6, 2009. opennet.org.

[40] Asher Moses. "Censoring Mobiles and the Net: How the West Is Clamping Down." *The Sydney Morning Herald*, August 15, 2011. www.smh.com.au.

[41] "Internet Filtering in China." OpenNet Initiative, June 15, 2009. opennet.net.

[42] Oliver August. "Staring Down the Censors." *Wired*, November, 2007.

[43] "IOC Agrees to Internet Blocking at the Games." *The New York Times*, July 30, 2008.

[44] Andrew Jacobs. "China Requires Censorship Software on New PCs." *The New York Times*, June 9, 2009.

[45] Edward Wong. "China Orders Patches to Planned Web Filter." *The New York Times*, June 16, 2009.

[46] Anurag Viswanath. "Green Dam on the Back Burner." *Business Standard (India)*, August 2, 2009. www.business-standard.com.

[47] Matthew Taylor. "China Drops Green Dam Web Filtering System." *The Guardian*, August 13, 2009. www.guardian.co.uk.

[48] Eason Jordan. "The News We Kept to Ourselves." *The New York Times*, April 11, 2003.

[49] Immanuel Kant. "What Is Enlightenment?" In *Foundations of the Metaphysics of Morals*, Upper Saddle River, NJ, 1997. Library of Liberal Arts.

[50] John Stuart Mill. "On Liberty." In *On Liberty and Utilitarianism*. Bantam Books, New York, NY, 1993.

[51] Edward G. Hudon. *Freedom of Speech and Press in America*. Public Affairs Press, Washington, DC, 1963.

[52] Francis Canavan. *Freedom of Expression: Purpose as Limit*. Carolina Academic Press, Durham, NC, 1984.

[53] Cass R. Sunstein. *Democracy and the Problem of Free Speech*. The Free Press, New York, NY, 1993.

[54] G. Steven Agee. *Jeremy Jaynes v. Commonwealth of Virginia*. Court of Appeals of Virginia, Record No. 062388, September 12, 2008.

[55] George Carlin. "Filthy Words." In *Occupation: Foole*. Atlantic Records, 1973.

[56] Supreme Court of the United States. *Federal Communications Commission v. Pacifica Foundation et al.*, 1978. 438 U.S. 726.

[57] "Spying on Kids' Internet Use." *CBS News*, February 2003.

[58] Associated Press. "Justices Uphold Use of Internet Filters in Public Libraries." *NYTimes.com*, June 23, 2003.

[59] Jeffrey Kosseff. "Libraries Should Bar Web Porn, Court Rules." *The Oregonian (Portland, Oregon)*, June 24, 2003.

[60] James Rachels. *The Elements of Moral Philosophy*. 4th ed. McGraw-Hill, Boston, MA, 2003.

[61] John Rawls. *A Theory of Justice, Revised Edition*. The Belknap Press of Harvard University Press, Cambridge, MA, 1999.

[62] Lorenne Clark. "Sexual Equality and the Problem of an Adequate Moral Theory: The Poverty of Liberalism." In *Contemporary Moral Issues*, McGraw-Hill Ryerson, Toronto, 1997.

[63] Langdon Winner. "Electronically Implanted 'Values'." *Technology Review*, 100(2), February/March 1997.

[64] Doug Johnson. "Internet Filters: Censorship by Any Other Name?" *Emergency Librarian*, 25(5), May/June 1998.

[65] "Teen Online & Wireless Safety Survey: Cyberbullying, Sexting, and Parental Controls." Cox Communications, May 2009.

[66] Mike Celizic. "Her Teen Committed Suicide over 'Sexting.' " *TodayShow.com*, March 6, 2009. www.msnbc.msn.com.

[67] Martin Dula. "Sexting: the Convergence of Two Revolutions." *Pop Culture History (blog)*. June 25, 2009. www.greathistory.com.

[68] Kim Zetter. "'Sexting' Hysteria Falsely Brands Educator as Child Pornographer." *Wired*, April 3, 2009. www.wired.com.

[69] "2009 Legislation Related to 'Sexting.'" National Conference of State Legislatures, July 27, 2009. www.ncsl.org.

[70] Dorothy E. Denning. *Information Warfare and Security*. Addison-Wesley, Boston, MA, 1999.

[71] States News Service. "FTC Testifies on Identify Theft, Impact on Seniors." July 18, 2002.

[72] Matt Richtel. "Financial Institutions May Facilitate Identity Theft." *NYTimes.com*, August 12, 2002.

[73] Javelin Strategy & Research. "2011 Identity Fraud Survey Report: Consumer Version." February 2011. www.javelinstrategy.com.

[74] Javelin Strategy & Research. "2009 Identity Fraud Survey Report: Consumer Version." February 2009. www.javelinstrategy.com.

[75] Jason Gertzen. "Protect Your Finances from Online Fraudsters, Experts Warn." *The Milwaukee Journal Sentinel (Wisconsin)*, December 8, 2003.

[76] David McGuire. "Bush Signs Identity Theft Bill." *WashingtonPost.com*, July 15, 2004.

[77] Federal Trade Commission. "Take Charge: Fighting Back Against Identity Theft," February 2005. www.ftc.gov/bcp/conline.pubs.

[78] Gartner, Inc. "Gartner Says Identity Theft Is Up Nearly 80 Percent," July 21, 2003.

[79] "Nielsen/NetRatings Finds E-mail Is the Dominant Online Activity Worldwide." *Nielsen/NetRatings*, May 9, 2002. www.nielsen-netratings.com.

[80] Lynn Burke. "Memoir of a Pedophile's Victim." *Wired News*, April 26, 2000. www.wired.com.

[81] Thomas Clouse. "Man Accused of Seeking Sex with 13-Year-Old Girl; Police Say Internet Sting Caught Suspect Who Had Handcuffs, Knife." *Spokane Spokesman-Review*, March 5, 2003.

[82] Shaila K. Dewan. "Who's 14, 'Kewl' and Flirty Online? A 39-Year-Old Detective, and He Knows His Bra Size." *The New York Times*, April 7, 2003.

[83] "Police Say Arkansas Man Made an Online Deal to Buy a Little Girl for Sex." *ZDNet UK*, September 3, 1999. news.zdnet.co.uk.

[84] "Chat Room Cops Nab Possible Predator." *Tech TV Inc.*, May 17, 2002. www.techtv.com.

[85] Paige Akin. "Man Arrested in Undercover Cyber Sex Sting." *Richmond Times Dispatch (Virginia)*, March 8, 2003.

[86] Suzannah Gonzales. "Sex Case May Lead to More Charges." *St. Petersburg Times (Florida)*, March 14, 2003.

[87] Jennifer Sinco Kelleher. "Arrests in Sex Chats with 'Girls.'" *Newsday*, March 15, 2003.

[88] Amy Klein. "Cops in the Chat Room; Detectives Play Teenagers to Bait Sexual Predators." *The Record (Bergen County, NJ)*, April 6, 2003.

[89] Joseph Weizenbaum. *Computer Power and Human Reason: From Judgment to Calculation*. W. H. Freeman and Company, San Francisco, CA, 1976.

[90] Andy Baio. "Finding the Star Wars Kid." *Waxy.org*, May 13, 2003. waxy.org.

[91] Tu Thanh Ha. "Parents File Lawsuit over Star Wars Video." *The Globe and Mail*, Toronto, Ontario, Canada, July 23, 2003.

[92] "Star Wars Kid Is Top Viral Video." *BBC News*, November 27, 2006. www.bbc.co.uk.

[93] Steve Pokin. "'MySpace' Hoax Ends with Suicide of Dardenne Prairie Teen." *Suburban Journals*, November 11, 2007. suburbanjournals.stltoday.com.

[94] "Parents Want Jail Time for MySpace Hoax Mom." November 29, 2007. abcnews.go .com.

[95] Kim Zetter. "Government's Star Witness Stumbles: MySpace Hoax Was Her Idea, Not Drew's." November 20, 2008. www.wired.com.

[96] "Missouri Begins Prosecuting Under Cyberbullying Law." *Fox News*, December 20, 2008. www.foxnews.com.

[97] Kim Zetter. "Lori Drew Not Guilty of Felonies in Landmark Cyberbullying Trial." November 26, 2008. www.wired.com.

[98] Kim Zetter. "Judge Acquits Lori Drew in Cyberbullying Case, Overrules Jury." www .wired.com.

[99] Congressional Research Service. "H.R. 1966: Megan Meier Cyberbullying Prevention Act (Summary)." April 2, 2009. www.govtrack.us.

[100] "Computer Addiction: Is It Real or Virtual?" *Harvard Mental Health Letter*, 15(7), January 1999.

[101] *Merriam-Webster's Collegiate Dictionary, Tenth Edition.* Merriam-Webster, Springfield, MA, 1994.

[102] Stanton Peele. *The Meaning of Addiction: Compulsive Experience and Its Interpretation.* Lexington Books, Lexington, MA, 1985.

[103] Kimberly S. Young. "Internet Addiction: Symptoms, Evaluation, and Treatment." *Innovations in Clinical Practice*, volume 17, edited by L. VandeCreek and T. L. Jackson. Professional Resource Press, Sarasota, FL, 1999.

[104] Mark Griffiths. "Does Internet and Computer 'Addiction' Exist? Some Case Study Evidence." *CyberPsychology and Behavior*, 3(2), 2000.

[105] Kimberly S. Young. "Internet Addiction: The Emergence of a New Clinical Disorder." *CyberPsychology and Behavior*, 1(3), 1998.

[106] John P. Charlton. "A Factor-Analysis Investigation of Computer 'Addiction' and Engagement." *British Journal of Psychology*, 99(3), August 2002.

[107] Aydrea Walden. "Center Helps Those Hooked on Internet." *The Seattle (WA) Times*, February 5, 2002.

[108] Jeffrey Reiman. *Critical Moral Liberalism: Theory and Practice.* Rowman & Littlefield Publishers, Lanham, MD, 1997.

[109] Immanuel Kant. *Lectures on Ethics.* Cambridge University Press, 2001.

[110] Matt Richtel. "Devices Enforce Silence of Cellphones, Illegally." *The New York Times*, November 4, 2007. www.nytimes.com.

[111] U.S. Department of State. "Internet Freedom." Fact sheet, February 15, 2011. www .state.gov.

[112] "Protesters Angry about Police Shooting Shut Down S.F. Subway Stop." *CNN*, July 12, 2011. www.cnn.com.

[113] "S.F. Subway System Admits Cutting Cellphone Service to Stop Planned Protest." *CNN*, August 13, 2011. news.blocks.cnn.com.