7

Responsible Online Communication

Kirk Hallahan

During the presidential elections in 2004, a wild rumor circulated throughout the United States that the federal government planned to reestablish a military draft. Fully one-half of all eighteen- to twenty-nine-year-olds surveyed in one public opinion poll said that they thought the rumor was true.

In fact, no such plans existed.

Many news reports attributed the rumor to the Web site and e-mail campaign conducted by an activist group called MoveOn.org Student Action. The group was an affiliate of a liberal activist group that had gained notoriety because of its efforts to unseat President George Bush and for its adroit use of the World Wide Web to raise political campaign funds online.

Similar to most rumors, the story about a prospective military draft was partly based on fact. In spring 2003, a full year before the invasion of Iraq, legislation had been introduced in Congress to reconstitute the military draft if needed. But leaders of neither major political party favored such a controversial action, even though presidential candidates John Kerry and Ralph Nader both made oblique references to the need for a draft in their campaign rhetoric.

The draft rumor thrived for several months while frustrated government officials tried unsuccessfully to squelch it. The agency that eventually would be responsible for registering prospective draftees was forced to post a message on its Web site that said, "Notwithstanding recent stories in the

news media and on the Internet, Selective Service is not getting ready to conduct a draft for the U.S. Armed Forces."[1]

Although another watchdog group, Congress2004.org, had conceived and championed the claim, MoveOn.org Student Action picked up on the antidraft argument and was successful in making the issue visible to a far larger audience because of its savvy use of the Internet.

New Frontiers of Ethics and Responsible Advocacy

In many ways, this incident illustrates the impact that the Internet has had in modern society. Web sites, e-mail, bulletin boards, newsgroups, chat rooms, and wireless telecommunications are now potent forces that must be reckoned with—and are being adroitly used by organizations ranging from loosely organized social movements to large Establishment organizations.

Yet, the effects of these new online media are not yet fully understood—and it is all too easy to fear, criticize, or overstate their impact. Indeed, the Internet was only one part—albeit an important one—in MoveOn.org's campaign to oppose continued military intervention in Iraq. Other activities included ads in college newspapers and special events on college campuses.

The Internet has transformed the techniques and technology of advocacy by enabling individuals and organizations with relatively modest resources to reach a global audience instantaneously twenty-four hours a day, seven days a week.[2] Many practitioners have embraced Internet technology,[3] while others have pointed to the Internet's potential to equalize power relationships in society and to provide a "voice" to otherwise marginalized groups.[4]

Yet, along with opportunity comes responsibility.

Once messages are created, the speed and ease with which online communications can be distributed, stored, duplicated, and redistributed pose new challenges for responsible communicators. In the case of the military draft rumor, for example, much of the "buzz" resulted from thousands of Internet users who forwarded e-mails and news stories to others. People also posted comments on message boards and Web logs (blogs) and forwarded links to Web sites that featured stories about a prospective draft.

Joint Statement of Principles on Public Relations and the Internet

Despite widespread adoption, surprisingly little attention has been paid in the professional public relations literature to the many ethical issues that confront public relations practitioners as users and operators of online communication systems. These include problems that are exacerbated in an

online environment (such as false claims) as well as a variety of ethical dilemmas peculiar to the Internet.[5]

For example, none of the codes of ethics promulgated by the principal professional organizations in the field—the Public Relations Society of America (PRSA), the International Association of Business Communicators, the International Public Relations Association, or the National Investor Relations Institute—specifically mention online communications.[6] Yet, all the organizations agree that the general principles embodied in their guidelines for professional conduct apply to practitioners who use the Internet.[7]

Since 2001, the principal source of guidance for public relations practitioners has been a somewhat obscure statement of ethical principles issued under the leadership of the Arthur W. Page Society, an organization of leading corporate communications executives. Members of the Page Society had become concerned about anonymous postings in chat rooms and bulletin boards, as well as the failure of practitioners to disclose the credentials of experts quoted online and potential conflicts of interest. The group worried that inaccurate or misleading information would lead to a loss of credibility for Internet communications.

The Page Society drew upon the classic principles outlined by the pioneer public relations professional for whom the organization is named, and obtained endorsements from ten other organizations for the resulting statement.[8]

Joint Statement of 11 Public Relations Organizations*

Establishing Principles for Public Relations on the Internet[9]

All public relations associations and news organizations share a common understanding for the need to adhere to ethical standards in communications with the public. Although statements of values regarding communications principles may take different forms, they are founded on certain basic tenets. Seek the truth. Minimize harm to others. Be accountable for your actions. Such unalienable principles are the underpinnings of honesty and fairness in everything we do as communicators.

As the newest communications tool, the Internet presents tremendous opportunities to build positive, productive relationships with a variety of publics. It also presents tremendous challenges to professional standards and ethical practices. The digital world is open and transparent. Erroneous or misleading information can be posted on the Internet and instantly and widely disseminated. Anonymity on Web sites can cause irreparable harm. The news media, which increasingly uses the Internet as an information

(Continued)

(Continued)

source, demands accuracy. Public relations practitioners risk losing credibility for themselves and their clients if they violate that trust.

The following principles, developed by the Arthur W. Page Society, are presented as a vehicle for public relations to attain and maintain the highest possible standards in the digital world.

1. Present Fact-Based Content

- Tell the truth at all times.
- Ensure timely delivery of information.
- Tell the full story, adhering to accepted standards for accuracy of information.

2. Be an Objective Advocate

- Act as a credible information source, providing round-the-clock access.
- Know your subject.
- Rely on credible sources for expert advice.
- Offer opportunities for dialogue and direct interaction with expert sources.
- Reveal the background of experts, disclosing any potential conflicts of interest or anonymous economic support of web content.

3. Earn the Public's Trust

- Simultaneously contact multiple stakeholders with relevant and accurate information.
- Disclose all participation in online chat rooms and conferences.
- Correct information that is online.
- Provide counsel on privacy, security and other online trust issues.

4. Educate the Public Relations Profession on Best Practices

- Compile case studies on the best use of the new media.
- Advance and encourage industry-wide adoption of best practices on the Internet.
- Practice principled leadership in the digital world, adhering to the highest standards.

---

*Organizations: Arthur W. Page Society, Corporate Communications Institute, Council of Communication Management, Council of Public Relations Firms, The Conference Board's Council on Corporate Communications Strategy, Institute for Public Relations, International Association of Business Communicators, Public Affairs Council, Public Relations Society of America, Public Relations Society of America Foundation, Women Executives in Public Relations. Adopted December 2001.

The joint statement was predicated on three ethical principles: practitioners should tell the truth, minimize harm to others, and be accountable for their actions. The joint statement identified fifteen guidelines for practitioners to follow in four broad areas: providing fact-based content, being objective advocates, earning public trust, and educating the profession.

Although the 2001 statement was a useful beginning, most of its tenets represent practical advice that ought to be followed whether practicing public relations offline or online. Among its few Internet-specific guidelines was the admonition that practitioners should avoid anonymous participation in chat rooms and discussions. In addition, the statement called on practitioners to become prepared to advise clients on ethical concerns such as online privacy, security, and trust. Although the statement called for the profession to develop and promote "best practices," no specifics for doing so were provided. And as of early 2006, no subsequent efforts have been undertaken by any of the participating organizations to do so. The statement is further limited because it carries no authority to monitor or enforce compliance.

Efforts Outside Public Relations to Promote Responsible Online Communications

The lack of emphasis on online ethics in the public relations field is partly explained by the fact that public relations practitioners use many communications tools, not just the Internet. Only two small groups within the field focus specifically on technology concerns: PRSA's Technology Section and the new International Association of Online Communicators.[10] Furthermore, many practitioners still view the Internet as a set of tools only for *outbound* communication. Most practitioners have been only minimally involved in the *inbound* collection of data from users—the greatest public concern about online ethics today.

Various initiatives outside public relations, stemming from both the private and public sectors, are shaping the standards of conduct for online communications. These are defining best practices and undoubtedly will influence future public relations practices.

Private-Sector Initiatives. Various organizations—ranging from the Catholic Church to local school boards—have issued position papers and policy statements related to online ethics.[11] Similarly, a number of professional and trade associations in fields ranging from appraising to medicine and psychology have incorporated provisions related to the Internet in their codes of conduct.[12]

Organizations whose members are directly dependent on online communications have taken the leadership to regulate themselves and to foster responsible online communications using four principal mechanisms:

Standards and guidelines have been promulgated by several of the leading trade associations in advertising and marketing. Examples include the American Marketing Association, the Interactive Advertising Bureau, and the Direct Marketing Association (DMA) in the United States; and the International Chamber of Commerce.[13]

The DMA's general guidelines, for example, address precautions about promotions to children and the collection, use, and maintenance of all user data. For its members involved in online marketing, the DMA outlines specific recommended disclosures that should be placed on Web sites to explain an organization's online practices. In addition, the DMA states that commercial e-mail solicitations should be sent to only a marketer's own customers, or people who have consented to receive mail and/or who have been given the opportunity to "opt out." The DMA also addresses the improper use of names referred by third parties without the permission of addressees. Finally, the DMA prohibits appending an individual's e-mail address to other electronic records unless specific requirements are met.[14]

Educational programs and organizations have been launched to promote ethical standards of conduct and public understanding of online communications. Many public relations practitioners work for organizations that subscribe to standards promulgated by these groups. Among the most prominent examples are the Electronic Frontier Foundation and the Electronic Privacy Information Center.[15] WiredSafety.org was created to help consumers protect themselves from abuse.[16] Other specialized groups include the Email Service Provider Coalition, the Coalition Against Unsolicited Commercial Email, and the International Council for Internet Communication—all formed to fight spam while protecting the delivery of legitimate e-mail. Meanwhile, the Network for Online Commerce has devoted itself to promoting ethical behavior among firms that provide paid entertainment and information services through telemedia worldwide.[17] Separately, the ePhilanthropy Foundation promulgated a Code of Ethical Online Philanthropic Practices.[18] Two examples in the health field include the Internet Healthcare Coalition and Internet Health Ethics (Hi-Ethics).[19]

A*ccreditation* programs for Web sites involve examinations by third-party organizations to ensure compliance with established guidelines.

Organizations whose Web sites pass scrutiny are permitted to display insignias designed to assure users that sites meet established criteria for protecting users and for maintaining content reliability. The two most prominent examples are Truste and iCop.[20] In the health arena, accreditation of Web health sites is conducted by URAC in the United States and by the Health on the Net Foundation worldwide.[21]

Professional certification or *credential programs* enable online communicators to demonstrate their knowledge, professionalism, and commitment to ethical conduct. Examples include testing programs sponsored by the International Association of Privacy Professionals and the Organization of Search Engine Optimization Professionals.[22]

Public-Sector Efforts. Public policymakers at the federal and state levels also have been pressed to guard against questionable online practices. The resulting rules for behavior contained in laws and regulations represent *minimum* standards of online conduct that organizations and individuals must follow to avoid civil or criminal prosecution.

In the United States, the communications activities of organizations can be regulated as part of the government's oversight of activities in which it has a *compelling state interest* as long as that regulation does not impose

Selected U.S. Laws Shaping Responsible Online Communications[23]

Fair Credit Reporting Act, 1970. Pub. L. 91–508, 15 USC 1601. Governs the collection and distribution of electronic credit reports. Strengthened most recently by the Fair and Accurate Credit Actions Act, 2003. Pub. L. 108–59, 15 USC 1601.

Family Educational Rights and Privacy Act, 1974. Pub. L. 93–380, 20 USC 1232g. Prescribed policies about the public disclosure of student information to be followed by educational institutions that receive federal funds.

Computer Software Copyright Act, 1980. Pub. L. 96–517, 17 USC 102, 117. Curtailed pirating by affirming copyright protection for computer software.

Computer Fraud and Abuse Act, 1986. 18 USC 1030(a). Prohibited unauthorized access to particular computer systems with intent to steal or

(Continued)

(Continued)

commit fraud. Strengthened in No Electronic Theft Act, 1998 Pub. L. 105–47, 17 USC 506.

Electronic Communications Privacy Act, 1986. Pub. L. 99–508, 18 USC 2510. Prohibited unauthorized access to specified electronic communications and disclosure of private communications.

Health Insurance Portability and Accountability Act (HIPAA), 1996. Pub. L. 104–191, 42 USC 1302(d). Outlined safeguards for protecting patient confidentiality, including electronic disclosures.

Children's Online Protection Act, 1998. Pub. L. 105–217, 15 USC 6501–650. Made it a federal crime to transmit harmful information to minors. Passed in response to the Supreme Court's overturning of the Communications Decency Act of 1996, Pub. L. 104–104, which had outlawed distribution of all online pornography. Complemented by the Protection of Children from Sexual Predators Act, 1998. Pub. L. 105–134.

Digital Millenium Copyright Act, 1998. Pub. L. 105–304, 17 USC 1201–1205. Extensively revised the Federal Trademark Act of 1947 (Lanham Act) to address digital media issues; guaranteed and protected the use of encryption systems.

Workforce Investment Act, 1998. Pub. L. 105–220, 20 USC 794d. Section 508 of the law requires that Web sites must be accessible to the disabled if paid for with federal funds.

Anti-Cybersquatting Consumer Protection Act, 1999. Pub. L. 106–113, 17 USC 1125 to strengthen the Federal Trademark Dilution Act, 1995. Pub. L. 104–98, 15 USC 1125c to protect against trademark misuse and dilution by others in an online environment.

Electronic Signatures in Global and National Commerce Act, 2000. Pub. L. 106–229, 15 USC 7001. Permitted and encouraged use of electronic signatures in commerce.

USA Patriot Act—United and Strengthening America by Producing Appropriate Tools to Interrupt and Obstruct Terrorism Act, 2001. Pub. L. 107–56, 28 USC 994(p). Expanded CPAA (1986) and provided exemption from prosecution for hardware, software, and firmware companies whose equipment might be used by terrorists. Allowed government to use wiretaps to monitor Internet users and permitted police to intercept communications of computer trespassers.

CAN-SPAM—Controlling the Assault of Non-Solicited Pornography and Marketing Act, 2003. Pub. L. 108–187. Authorized the FTC to curtail delivery of undesired commercial messages.

undue prior restraint on free speech. An examination of the debates leading up to the adoption of each of these laws and regulations is informative because advocates invariably called for legislation and regulation based on public concern and examples of egregious violations of the public's expectations about ethical behavior.

Administrative regulations also are beginning to subtly influence how organizations conduct online activities. For example, the Federal Trade Commission (FTC) promulgated an advisory to businesses that effectively places Web site designers in the same category as advertising agencies. Both groups are now responsible for reviewing online information to substantiate claims and to avoid information that is misleading. To help Web site sponsors determine whether required disclosures are clear and conspicuous, the FTC provided a series of guidelines for ethical communication. According to the FTC, disclosures should be in close proximity to relevant claims or should be easily found through the use of clearly labeled markers and links; disclaimers must be prominent and not overshadowed by distracting material; audio messages must be presented with adequate volume and cadence to be heard; visual disclosures must appear for a sufficient duration; and the language used needs to be understandable by the intended audience.[24]

A second federal agency, the Food and Drug Administration (FDA), is also concerned with unethical online activity, particularly misleading claims and outright fraud involving the sale of drugs and medical devices. (The agency is still formulating a position about whether drugs ought to be sold online at all.) Unlike the FTC, the FDA has issued no specific guidelines related to the production of online content. However, the agency routinely issues "cyber letters" to Web sites believed to engage in questionable activities. The FDA also encourages legitimate Web site operators to display public service messages (banner and button ads) that lead consumers to precautionary information on the FDA's site.[25]

Separately, the Securities and Exchange Commission (SEC) proactively encourages use of the Internet to meet its mandate that publicly traded companies engage in prompt and full disclosure of material information that could influence investment decisions. Since 1984, the SEC has required the electronic submission of SEC filings by regulated companies. In 2002, the agency broadened the list of material information that should be provided on company Web sites, either directly or through links to the SEC's Electronic Data Gathering and Reporting (EDGAR) system. At the beginning of 2005, the SEC promulgated proposed rules that would change the procedures for initial public offerings (IPOs). The SEC proposed that

companies be allowed to use Webcasts to distribute analyst presentations ("road shows") to a broad array of audiences and to forego distribution of final offering prospectuses if the documents were available online.[26]

Ethics and Computing: A Broader Perspective

As computing became increasingly prominent in people's lives during the twentieth century, computer engineers and operations professionals found themselves grappling with the questions of ethics and social responsibility.[27] In part, this reflected the increased sense of professionalism among computing professionals and culminated in the adoption of a joint code of ethics by two of the largest computer associations, the Association for Computing Machinery and the Institute of Electrical and Electronics Engineers.[28] Other specialized organizations were formed, such as the Computer Ethics Institute, an affiliate of the Brookings Institute in Washington, D.C. The Computer Ethics Institute, most notably, published a widely quoted "Ten Commandments of Computer Ethics."[29]

Ten Commandments Of Computer Ethics[30]

1. Thou Shalt Not Use A Computer To Harm Other People.
2. Thou Shalt Not Interfere With Other People's Computer Work.
3. Thou Shalt Not Snoop Around In Other People's Computer Files.
4. Thou Shalt Not Use A Computer To Steal.
5. Thou Shalt Not Use A Computer To Bear False Witness.
6. Thou Shalt Not Copy Or Use Proprietary Software For Which You Have Not Paid.
7. Thou Shalt Not Use Other People's Computer Resources Without Authorization Or Proper Compensation.
8. Thou Shalt Not Appropriate Other People's Intellectual Output.
9. Thou Shalt Think About The Social Consequences Of The Program You Are Writing Or The System You Are Designing.
10. Thou Shalt Always Use A Computer In Ways That Insure Consideration And Respect For Your Fellow Humans.

Computing professionals quickly recognized their need to be accountable and have largely rejected the notion of what the author Richard T. DeGeorge calls the "myth of amoral computing and information technology." Computers obviously are not moral beings; people clearly are responsible for the design, function, and consequences of technology.[31] Yet, as social critics—including Jacques Ellul, Neil Postman, and others—have pointed out, modern societies embrace new technologies almost unquestioningly and without considering the moral and social consequences.[32]

The increased reliance on communications technology results from both increased demand for information and the slavish promotion of new technologies, motivated by the desires for productivity among users and for profitability among suppliers. These two "pull" and "push" forces have multiplied the "moments of truth" where people make critical decisions about how technology will be used.[33]

In principle, online communications are no different from any other human activity. However, the Internet features some peculiar characteristics that pose particular ethical challenges. These include its instantaneous speed, global scale, anonymity, interactivity, reproducibility, and uncontrollability.[34] One leading Internet ethicist, Jerden van den Hoven, suggests the application of traditional applied ethics is inadequate in the age of cyberspace. He cites the loss of territorial base for comparison when making judgments, the redefinition of moral concepts, problems in attributing responsibility, and ignorance among both computer operators and users about the consequences of their actions.[35]

A widely cited expert, Lawrence Lessig, argues that regulation of cyberspace is driven as much by the architecture of Internet technology itself (the "code") as by laws, the market, and social norms.[36] But Richard Spinello, a leading ethicist who specializes in technology issues, argues that ethics are more than merely social norms. Instead, Spinello contends that ethics serve as *metanorms* that represent universal values that ought to play a directive role in influencing all the factors Lessing cites—laws, the market, system architecture, and social norms.

Spinello organized the moral quandaries in the electronic frontier into three categories. He suggested the following operative moral questions:

> *Consequences-based morality:* Which action or policy promotes the best overall consequences or the greatest utility for all parties?
>
> *Duty-based morality:* Can the maxim underlying the course of the action being considered be universalized? Is the principle of fair play being violated? If there appear to be conflicting duties, which is the stronger duty?

Rights-based morality: Which action or policy best protects the human and legal rights of the individuals involved? Does the proposed action or policy impede the basic requirements of human flourishing?[37]

Spinello's model reflects major approaches to ethics commonly cited in the public relations literature and elsewhere.

Consequences-based ethics involves, among other things, the principle of *enlightened self-interest* (also known as *egoism*), which suggests that an action is morally right if it promotes a party's long-term interests.[38] Thus, the operator of a Web site might think a particular practice is justified if it results in online traffic or transactions. Consequences-based ethics also incorporate a *teleological* approach to ethics, which suggests that the obtained result is what's important. *Teleos* is the Greek word for "the good" or "the end." Using this rationale, the end justifies the means because the benefits exceed the costs. This is particularly true if the results produce happiness, pleasure, or the greatest social good. The utilitarian ethical approach, first suggested by writers such as John Stuart Mill and Jeremy Bentham, might suggest that knowingly deceptive online practices are acceptable because they contribute to attaining larger, even socially desired, goals.[39]

Duty-based ethics are grounded in *deontological* ethics, which rejects utilitarianism and argues that people must employ proper means and act with good intentions regardless of outcomes. *Deontology* is based on the Greek word *deon,* for "duty" or "obligation." The philosopher Immanuel Kant popularized this idea in his notion of the *categorical imperative,* in which he argued that all human actions must be fair and honest.[40] Judeo-Christian and other cultures around the world embrace the notion that people are not merely means toward ends and emphasize values such as respect for the individual, choice, freedom, and justice. A number of modern-day ethicists have outlined typologies of the values that thus constitute ethical behavior.[41]

Rights-based ethics go beyond deontological obligations to emphasize that people are *entitled* to fair and equitable treatment. One approach, which was popularized by Joseph Fletcher in the 1960s, argues that ethics are rooted in the notion of *community.* These ethicists argue that ethical maxims (or expectations) vary by community and are not absolute—although love, human welfare, and happiness appear to transcend most communities as bases for ethical decision making.[42] Another example involves *communitarianism,* which has received attention as a possible framework for public relations.[43] Similarly, *distributive justice* draws upon the notion of the contractual rights that exist between the individual and civil society. The philosopher John Rawls suggested in the 1970s that people often operate in a "veil of ignorance" and don't fully understand their position in a social system or their own capabilities. As a result, a moral society must consider the

needs and rights of all members. Justice requires that people have (a) equal claim to basic rights and liberties, and (b) equal access to opportunity.[44]

Although all of these approaches to ethics might be applied to groups or organizations seeking to conduct responsible online communications, the latter-day approaches based on duty and rights—and that emphasize community, respect, and equal access—have particular appeal. This is especially true when considering the contemporary emphasis on Internet users as a *virtual community*.[45]

One application of this rights-based approach is the call for a *new social contract* to govern our information society. The information ethicists Richard Mason, Florence Mason, and Mary Culnan identified six key tensions that provide a framework for considering ethics in an information management context. These included ownership and use of intellectual property, privacy, the quality and accuracy of information, information justice (access), gatekeeping (restrictions on the free flow of information), and technological implementation that avoids social disruption, dislocation, and human misery.[46]

According to Mason, Mason, and Culnan, four parties play principal roles in the information society: *Information givers* provide information. *Information orchestrators* gather, process, store, and disseminate information and serve as information gatekeepers. *Information takers* receive and use information for their own purposes. (In a public relations context, clients are information takers whereas practitioners often serve as information orchestrators). Finally, *stakeholders* are people (and organizations) affected by the information-based actions in which information takers engage. The responsibilities of each can be summarized as follows:

- Information takers should collect information only for legitimate purposes that are just and beneficial to givers and to stakeholders.
- Information takers and orchestrators should use the information only for the purpose for which it is taken and obtain consent from givers.
- Information givers ought to supply the source information because it is necessary in order for takers to take action or benefit shareholders.
- Information orchestrators or gatekeepers should handle information with fidelity to source while shaping, limiting, or expanding it to best meet the takers' needs.[47]

Eight Core Concerns: A Framework for Ethical Online Public Relations

Thus far, this chapter has examined the limited effort to delineate principles of responsible online public relations. It also reviewed steps taken in the

private and public sectors to curb abuses and foster responsible online communication more generally. Finally, within the emerging context of information management, it has explored key concepts in ethics.

Ethics in public relations (or any other activity) can be defined as establishing and following criteria to be used when making decisions about what is right or wrong.[48] The late Supreme Court Justice Potter Stewart, in a frequently cited quote, defined ethics as "knowing the difference between what you have the right to do and what is the right thing to do."

Importantly, ethics are *social constructions* that are negotiated. People concerned with particular social problems (such as abusive online practices) come to agree on what are accepted rules through a process of deliberation. Indeed, Aristotle's principle of the "golden mean" suggested that in every situation there are two extremes and that the ethical choice is in the middle.[49]

The remainder of this chapter integrates these various ideas by identifying eight broad areas of ethical concerns for online public relations practitioners. The discussion identifies overarching areas of concern, but also points out particular practices that are problematic. Importantly, defining ethical online behavior is an ongoing process, and acceptable standards of practice continue to evolve.

Access and Choice

Ethical online public relations begins by providing publics with the opportunity to communicate. A decade following the popularization of the Internet, people have come to *expect* that organizations and groups have an online presence and that users can communicate with them online if they choose to do so.

Access involves offering users the choice of tools (Web sites, e-mail, newsgroups, games, etc.) and delivery options that best meet their needs (personal computers, wireless, personal digital appliances, interactive television, etc.). In the coming years, this will require organizations to make an increased commitment of resources to offering a variety of access options.[50]

Despite the ostensibly ubiquitous presence of the Internet, only two-thirds of Americans have Internet access, and adoption rates vary considerably based on age and socioeconomic status. Penetration rates also differ widely worldwide. The public debate about this "digital divide" requires public relations practitioners to be sensitive to problems of equal access consistent with duty- and rights-based approaches to ethics. In a few instances, such as the promotion of topics inappropriate for children, access might need to be limited on ethical grounds.

Moreover, not all constituents necessarily will *want* to use the Internet in every situation to communicate with an organization. Despite efforts to be on the cutting edge (and to reduce costs by shifting constituent contact to the online environment), prudent organizations must continue to allow (and encourage) alternative forms of contact—the telephone, correspondence, and personal visits—if they are truly committed to serving constituents. In short, giving people *choices* is important.

Accuracy of Content

Ethical online public relations cannot be misleading. Depending on the circumstances, content might be subject to governmental oversight (by agencies such as the FTC, FDA, or SEC in the United States) to guard against fraud. However, content needs to be accurate, complete, and current to maintain the confidence and trust of users—as a matter of duty and users' rights.

Public relations practitioners must be vigilant about the accuracy of content, whether produced by a public relations unit or others in their client organizations. The broad and rapid-speed dissemination of information requires practitioners to avoid distributing inaccurate information that can be stored, reproduced, and redistributed unwittingly by recipients who assume the veracity of information. The real-time nature of the Internet allows for the easy updating of information on Web sites and e-mails. Ethical practice requires making every effort to correct and acknowledge errors quickly.

Accuracy applies to both verbal and visual messages. One of the unintended consequences of new digital technologies is the ability to digitally manipulate photos and graphics. Although photographers and graphic artists have always employed a variety of techniques to enhance pictures, electronic editing systems now make it tempting for practitioners and others to alter the *material* accuracy of images and thus alter the representation of reality. This problem is further exacerbated on the Internet because intermediaries and end users have the same capabilities to alter images.[51]

The fragmented and decontextualized nature of online communications (evidenced by the layering of content on multiple Web pages and people's propensity to use cryptic language and sometimes ambiguous references in e-mails) demands that each communication be complete so it can be understood on its own.

Also of concern is the consistency of messages—an important contributor to a message's believability. Online communications must engender verisimilitude (a sense of realism) and resonate with a person's offline experience. To do otherwise can mislead audiences, interrupt message processing,

or discourage message acceptance. A lack of believability raises doubts about the trustworthiness of the message, the source, and online communications itself. Thus, public relations practitioners are posed with new responsibilities to monitor their organization's online presence as a critical element in reputation management.

Deceptive Practices

Ethical public relations involves the avoidance of deceptive practices related to the design and functionality of online communication. Practitioners can unwittingly engage in deception whenever otherwise accurate information is presented in a way that misleads users.

Obvious examples of unethical conduct include the *misappropriation* of content from another source. Practitioners must not misrepresent themselves by using the intellectual properties of others. This includes reproducing copyrighted material without acknowledgement or beyond the established rules of fair use. This also includes reproducing editorial matter from newspapers and magazines that favorably mention a client, unless permission is granted and it is clearly labeled. Similarly, practitioners should not use another party's trademark unless authorized and permission to do so is acknowledged.

In the case of Web sites, more subtle ethical problems involve including textual links to another's Web site without permission and using screen frames to enclose another organization's Web pages within another without permission. The effect of these techniques is to suggest an endorsement or relationship that might not exist.

Deception also can occur in the layout of Web pages, where information is so fragmented that it becomes difficult for a user to fully comprehend the context in which an idea or offer is presented. As the FTC's guidelines suggest, material disclaimers must be both in close proximity and sufficiently prominent so that users are not misled. Users also can be deceived into thinking that they have no other option for communicating with an organization when addresses, telephone numbers, and e-mail addresses are omitted.[52]

Deceptive misrepresentation of online sources is probably the most egregious ethical problem in the online environment today. Not identifying a source and using false-front organizations (where the real identity of sponsors is purposefully withheld) are prohibited under the PRSA Code of Ethics. However, many organizations operate online without fully disclosing their identity, which places a burden on users to check the veracity of information and sources.[53]

Participating in chat rooms and bulletin boards without identifying one's connection to an organization that might have a vested interest in a topic under discussion is one of the few ethical violations specifically identified in the "Joint Statement on Public Relations and the Internet." However, a more difficult question is whether a chat room participant should even eavesdrop on conversations. Some proponents of this practice argue that monitoring discussions is the legitimate equivalent to watching a public debate or employing an electronic clipping service. On the other hand, critics of the practice point out that many chat rooms are considered private conversations among participants in a community of common interest. Depending on rules that might explicitly be stated when registering, or that might be implicitly understood by participants, lurking in chat rooms to collect intelligence could be an unethical breach of duty or the violation of the rights of participants.[54]

Other identity-related problems involve the branding of Web sites. Competitors or opponents often create sites with similar names (such as whitehouse.com versus whitehouse.gov). These *rogue sites* (which include *attack sites* as well as *spoof sites*) divert traffic from legitimate site operators for financial or political gain. Although such sites are legal as long as they do not create initial confusion of intent, such branding practices are questionable. Similarly, purchasing Web addresses so that legitimate potential users cannot use them (or must purchase the rights to do so at a hefty charge) has been labeled *cybersquatting*—an unethical practice that is now illegal in the United States.[55]

Tracking technologies that might be used by a client organization similarly give rise to ethical issues. The least invasive of these involve the use of *cookies,* short fragments of identifying computer code placed on a user's computer in order to track and facilitate future Web site use. Cookies are a somewhat questionable form of attendance taking, but have become generally accepted because computer users can alter the settings on their Web browsers to not accept cookies. A more invasive and clearly questionable practice is the placement of *adware* or *spyware,* software remotely installed without permission, on a user's computer. The intent is usually to track Web site visits and to then direct compatible content to the users. But spyware can also be used to eavesdrop on correspondence, steal electronic files, or even disarm or disable computers.[56]

A growing, but less known, set of deceptive practices involves manipulating the prominence with which sites are listed on search engines (euphemistically referred to as *search engine optimization*).[57] Yahoo!, Google, and other search engines now generate considerable advertising revenue through "featured site" programs where sponsors pay for prominent placement.

However, such financial arrangements are not readily evident nor disclosed to users. Public relations practitioners ought to question whether their client organizations want to engage in this kind of Web site promotion, which relegates Web sites to being perceived merely as advertising.

Other unscrupulous activities involve tricking the *remote agent software* (also known as *crawlers, spiders, ants, robots,* and *intelligent agents*) that search engines deploy to catalog content on the World Wide Web. Web site operators are stuffing extra or inappropriate keywords in metatags, inserting hidden text and links that are read by the search engines but are invisible to users, employing *bogus referral pages* to inflate visitor counts, and using *cloaked* pages where Web sites serve up one page to a search engine for indexing and another to users.[58] All are efforts to make Web sites appear to be more popular than they really are—and thus more relevant to searchers and attractive to advertisers.

Deception can occur when paid content appears on other Web sites. Besides search engines, there has been a recent trend toward the use of undisclosed product placements on Web sites, which reflects the more general ethical problem that hybrid messages represent in movies and on television.[59] Since 2000, the American Society of Magazine Editors (ASME) and the Magazine Publishers Association have promulgated voluntary guidelines designed to differentiate editorial matter from advertising and "sponsored content." Among ASME's eight standards, all online magazine pages should disclose whenever an advertiser pays for a link embedded in editorial content, *advertorial* sections should be clearly labeled as such, and e-commerce and other affiliate fees should be reported on a disclosure page.[60]

In a similar way, the posting of patently promotional messages on computer bulletin boards and on opinion blogs (known as splogging) and the distribution of promotional messages via e-mail (spamming) and instant messaging (spimming) have generated outcries about deception, particularly when the identity of the sponsor is not disclosed.

Dependability

Ethical online communication is dependable. People with Internet access increasingly rely on online information to make critical decisions and to flourish in their personal lives. Thus, sponsors and operators of online systems have a duty to meet people's performance expectations, if not a responsibility to fulfill their right to information. Responsible online public relations practitioners also must concern themselves with reliability issues.

Dependability includes twenty-four-hour access, timely updates, a minimum of downtime, and the proper functioning of software and hardware.

Dependability is particularly critical during crises, the time of uncertainty that follows natural disasters or other extraordinary events. People naturally seek up-to-date and accurate information about how the crisis might affect them and what actions they should take to avoid risks. Ethical PR practice requires organizations to anticipate such circumstances and to prepare for them.[61] For example, many crisis response teams now include online communications specialists. Crisis plans now include alternative methods to provide Web and e-mail access during system outages or during periods of high demand following extraordinary events. These techniques include maintaining backup or off-site computer servers known as *hot sites*.

Interactivity and Involvement

Ethical online public relations takes maximum advantage of the inherently interactive nature of online communications.

Among all the communications tools available to public relations practitioners, online communications are uniquely equipped to allow organizations and their constituents to engage in *two-way* communications. Normative theories of public relations practice equate ethical behavior with the degree to which organizations engage with and involve their publics. The ideal and most ethical model of public relations practice is posited to involve *symmetrical* communication, in which the organizations and constituents share power and interact on an equal basis.[62] This approach has also been defined as engaging in dialogue. A growing line of research has considered how Web site designers can improve *dialogic* characteristics of Web sites and online communication.[63]

Ethical online communications encourage users to become active participants in the communication process.[64] *System interactivity* empowers users to control the online experience itself—by selecting content and choosing to use features inherent in the system. *Verbal interactivity* enables users to express themselves—through written words (e-mail, newsgroups and chats, and fill-in/feedback forms on Web sites), spoken words (*online audio* and *Web conferencing*), and visual images (including personal *Web cams* used in instant messaging, *Webcasting,* and the sharing of *digital images*).

Responsible organizations that invite verbal interaction must be prepared to respond in timely and meaningful ways when users communicate opinions, ask questions, or request information, products, or services. Effective and ethical responses involve prompt acknowledgement of inbound messages, personalized (versus generic) answers, and the timely fulfillment of requests.

In addition to promoting dialogue *between* an organization and its constituents, organizations also can facilitate conversations *among* members of

stakeholder groups. Tools can include interactive chats, bulletin boards and newsgroups, and Web conferences on the public Internet or limited-access intranets (for employees) or extranets (for suppliers, distributors, or allied organizations). By capitalizing on such tools, public relations practitioners and their client organizations can foster a sense of community.[65] However, such efforts can only be successful (and ethical) if they encourage and foster the free expression of ideas. This requires tolerance for comments that challenge or question an organization's policies or practices and the elimination of fears about reprisals. At the same time, however, sponsorship of such activities also places upon sponsoring organizations the ethical responsibility to police users' actions that might be abusive, dangerous, illegal, or threatening to other participants.

Personalization and Customization

Ethical online public relations takes advantage of personalization and empowers users to shape their online experience through customization—features of online communications that public relations practitioners have yet to fully exploit.

One of the great strengths of online communications, particularly Web sites, is the ability to tailor information to the needs and interests of users. *Personalization* entails providing information based on the known interests or characteristics of a user. *Customization* enables users to knowingly select and organize categories or channels of content based on their interests. Examples of customization include the "My . . ." tab found on some commercial Web sites and portals set up on organizational intranets.

However, personalization raises ethical concerns regarding both how information is obtained and how information is used. Many organizations *ask* users to complete registration forms or surveys that give users the option to receive or not receive particular kinds of information ("opt-in" or "opt-out"). Some systems, however, tailor the information provided by tracking and recording the user's online behaviors. Online merchandisers, for example, use cookies to impute a user's interest about particular categories of products based on searches conducted or visits to particular topical areas—and then prominently promote related merchandise. Beyond the fact that the user was not asked, the result can often lead to erroneous or potentially embarrassing assumptions.

Customization, while presumably rooted in actual choices made by the user, can also raise ethical questions. Most customization systems limit the choices that can be made to a range of options prescribed by an organization and prohibit certain forms of content from either being customized or even being accessible. In the workplace, for example, access to pornographic

Web sites or e-mail flies in the face of providing people with a choice of content and raises the perplexing questions of when such limitations are appropriate and ethical.

Both personalization and customization raise ethical concerns about how data and systems settings might be used to *profile* users—a form of electronic stereotyping. Profiling clearly is illegal if used to discriminate against a user based on race, color, creed, religion, national origin, or marital status. However, people are often unaware of when their rights to equal opportunity are violated. Other data, such as age, education, or income, might appropriately be used as a basis for segmenting audiences. However, audience segmentation based on personalization or customization (or other online behaviors, such as visits to pornographic sites or sites advocating the overthrow of a government) also are wrought with potential problems of discrimination, recrimination, or reprisals in violation of a user's rights.

Privacy and Security

Ethical online public relations respects user privacy and maintains data security. Both privacy and security involve guarding the confidentiality of *personally identifiable information* about users.

Privacy focuses on the questionable use of provided or imputed personal information by an organization itself. *Security* involves the potential theft and/or misuse of the data by others (such as computer *hackers* or unscrupulous employees) who might gain unauthorized access as a result of breaches in an organization's systems.

Nearly two-thirds of Americans have expressed serious concerns about online privacy.[66] Consumers fear they can be harmed, embarrassed, disadvantaged, or annoyed. Organizations that collect data are expected by users (and watchdog groups and lawmakers) to exercise care in using information available to them about users. Special care is required when collecting data from protected classes, such as children, but the problem applies to all users who might be treated unfairly.

With increased frequency, public relations practitioners are asking for personally identifiable information from users. Requests might be as simple as asking a journalist to register in a pressroom or to provide an e-mail address in order to receive news releases or electronic newsletters via e-mail. However, many general queries from consumers and citizens also ask for name and contact information that are stored in an organization's database. More detailed information is frequently acquired from users such as donors, customers, or employees.

Public relations practitioners must examine both the policies and practices of their own units and of their organizations to consider the establishment

of formal guidelines, such as those recommended by other groups in the field.[67] Although the specifics may vary, ethical online database management involves providing *notice, choice,* and *redress*.

Notice usually involves providing a privacy statement on Web sites or in initial e-mails that discloses the nature of information that might be requested and how that information will be used. Although sometimes implied, ethical organizations should provide an explicit promise that information will be used only for the purpose for which it was obtained and that the organization will exercise care to protect all information provided.

Choice involves giving people the option to provide or not provide personally identifiable information or to put limits on how data about them are be used. For example, some users might not object to receiving future e-mail communications. Yet the same users might object to the sharing of data with third parties (including an organization's public relations consultant!).

Redress entails maintaining procedures so users can know about and correct errors in whatever information about them might be in an organization's files. Ethical organizations are also obligated to publish and to follow established procedures to quickly and appropriately disclose and remedy breaches of privacy.

These principles of notice, choice, and redress make sense, but also are consistent with public relations principles related to duty and the rights of publics on whom a group or organization depends for its success. Not surprisingly, public concern about online privacy and security has evolved into a major public issue that public relations practitioners must address on behalf of clients in their dealings with consumers, the media, and government.

Usefulness and Usability

Finally, ethical online public relations involves supplying meaningful content in a functional format that is usable by both novice and experienced online users.

Usefulness and usability are important if only to improve the communications effectiveness between an organization and the user constituents. For that reason, the U.S. Department of Health and Human Services has launched an initiative to improve the effectiveness of online health communications by promoting usability standards. Yet, providing information that is pertinent and relevant (through techniques such as personalization) also contributes to user satisfaction and the quality of the online experience—a right to which users might be entitled ethically.

Research on usability suggests that content is critical to assessments of satisfaction by users. However, Web sites, cellular phone screens, and personal data appliances (PDAs) also should feature functional designs that

are easy to navigate so people find the information they need with a minimum of errors.[68] Special accommodations are required to serve the growing number of online users who might suffer from disabilities, and practitioners can confirm that Web sites comply with established standards using HTML validator software.[69]

Conclusion

From this discussion, it is readily apparent that a wide range of ethical concerns confront public relations practitioners who use online communications. Many of these concerns focus on protecting individuals as matters of duty. Others are based on the rights of users. Clearly, the Internet is here to stay as a fixture in modern life, and organizations and users alike must adapt to the changing technologies. Both must learn and develop trust about new ways of communicating while discerning what constitutes ethical practice.[70]

Adhering to this burgeoning array of ethical concerns is a daunting task. However, any discussion of ethical online public relations also must take into account problems created for organizations by the unethical actions of users. Organizations, groups, and causes of various kinds are themselves the targets of unethical and unscrupulous detractors and competitors who will take whatever action they can to resolve a dispute or promote a cause. Ethical online behavior is a matter of good citizenship in a democratic society. But abuses can take place in the form of attacks, libelous or scandalous accusations, hate speech, fraud, misrepresentation, subterfuge, and stealing of intellectual properties. Scoundrels can be classified as attackers, hackers, lurkers, rogues, and thieves.[71] Practitioners must become aware of this "dark side" of online ethics and take steps to protect their organization's reputation and other digital assets in cyberspace.

As an activity that inherently attempts to influence people's behavior—what they know, how they feel, and why they act—public relations practice is inextricably intertwined with ethics. The motives of organizations in general (and public relations in particular) are continually called into question. As a result, public relations practitioners must strive for professionalism and high standards of ethical practice online.

But defining what is ethical is sometimes difficult in a rapidly changing environment where traditional benchmarks do not apply. Similarly, as Lawrence Lessig suggested, the forces of the marketplace, technology, and social norms are reshaping how online public relations will and ought to be conducted.[72]

Elsewhere, I have drawn on earlier public relations theory[73] to argue that online communications can help build organizational-public relationships.

In that context, key outcomes that shape ethical online communications include perceived *commitment,* a shared sense of *communality, mutual control* of the relationship, *satisfaction,* and *trust.*[74] To the extent that online public relations practices contribute to achieving these relationship-based outcomes, they can be deemed ethical.

Public relations practitioners must be concerned with both the ethical conduct of the public relations unit itself as well as the ethical online conduct of the entire organization and anyone involved in helping an organization achieve its goal. This is particularly critical because online communication, such as the operation of a Web site, is a *shared* organizational activity where responsibility transcends individual organizational units such as marketing, operations, human resources, or public relations. Online stakeholders do not differentiate between different parts of an organization when their only frame of reference is a Web site or bulletin board. Even more so than in an offline environment, organizations must speak responsibly with a "single voice" in cyberspace.

Table 7.1 Useful Web Resources on Ethics and Responsible Online Communications

Centre for Democracy and Technology	www.cdt.org/
Computer Ethics Institute	www.brook.edu/its/cei/cei_hp.htm
Computer Scientists for Social Responsibility	www.cpsr.org/
Direct Marketing Association	www.the-dma.org/
Electronic Frontier Foundation	www.eff.org/
Electronic Privacy Information Center	www.epic.org/
ePhilanthropy Foundation	www.ephilanthropy.org/
Ethics Resource Center	www.ethics.org/
Internet Healthcare Coalition	www.ihealthcoalition.org/
U.S. Department of Health and Human Services	www.usability.gov/
U.S. General Services Administration	www.section508.gov/
Online Ethics Center for Engineering and Science	www.onlineethics.org/
PR-education.org	pr-education.org/onlineethics.htm
Society of Technical Communication	www.stcsig.org/usability/topics/ethics.html
Wired Safety	www.wiredsafety.org/