

# Ethics Online

*Shaping social behavior online takes more than  
new laws and modified edicts.*

Deborah G. Johnson

**N**ATIONS AROUND THE WORLD ARE IN THE process of making fundamental decisions about the future of their systems of online communication. The public discussions taking place are revealed in the visions of the future that are being put forth. In the U.S., we have Vice President Al Gore using the metaphor of “electronic superhighways of the future” and seeing a national and global information infrastructure as the means by which the U.S. will emerge triumphant in global economic competition. We have John Barlow, Mitch Kapor, and the Electronic Frontier Foundation using a highly gendered metaphor of the new frontier—cyberspace—in which thugs, overzealous sheriffs, and the pioneers of the 21st century are fighting it out. We have visions of a new form of democracy emerging online as political alliances are formed and social movements gather force without mediation from mass media.<sup>1</sup> We have visions of this evolving technology bringing into our homes the ultimate in entertainment choice together with the efficiency of being able to carry on all of our daily interactions with keystrokes and screens, such as shopping, working, job searching, and banking, among so many others.

The visions sometime include the possibility of escape into Disney-like virtual worlds. These are all highly value-laden and interest-laden visions competing for our attention. While they are all possible, none of them is inevitable. Rather, they work as self-fulfilling prophecies: The vision we embrace will shape what we make of online communication.

Online communication has been evolving and growing

<sup>1</sup>One documented example is the protest against Lotus Development Corp.’s product Lotus Marketplace: Households. It was a CD-ROM marketing database containing information on 120 million U.S. citizens. The announcement of the product eventually led to Lotus’s receiving thousands of letters from people requesting their names be removed from the database. Much of this was done via email directly to Lotus [4, 11].

at an unprecedented pace, and there is every indication the demand for it will continue. Its evolution, however, has not been without problems and the most disturbing of these involves human behavior. Disturbing and disruptive behavior ranges from unauthorized access, theft of electronic property [8], launching of destructive worms and viruses [1], racism, defamation [2], and harassment to an incident involving a form of online rape [3]. Our responses to this behavior will shape the future of online communication and will determine to what extent and in what ways the promise of electronic networking technology is realized in the future.

Our primary responses to behavioral problems online have so far been legal and technological. As problems have been identified and defined, laws have been extended or created, and law enforcement has entered this new domain [1]. We have new technologies for virus detection and for encryption and decryption of information. Our knowledge of how to secure our systems and detect or trace transactions has improved.

These approaches alone, however, will never be adequate to control online behavior. Our only hope is for individuals to internalize norms of behavior. That is how most behavior is controlled offline. Individuals implicitly understand that certain behavior is unacceptable, undesirable, or inappropriate, and they act accordingly. To achieve this, it is important that we discuss the character of online behavior and reveal its underlying meaning and the reasons for declaring it acceptable or unacceptable, desirable or undesirable, right or wrong, legal or illegal. Users must become aware of the meaning and consequences of their actions.

The issues and problems in electronic networks are the problems of the world around them. They have to do with who we are and what we do offline. The problems are the problems of modern, highly industrialized, democratic societies. Computer technology did not come into being in

a vacuum. It was created and shaped in response to pushes and pulls in our way of life—culture, politics, and social institutions.

The ethical issues surrounding computers are new species of generic moral problems [5]. This is as true when it comes to online communication as it is in any other area of computing. The generic problems involve privacy, property, drawing the line between individual freedom and (public and private) authority, respect, ascribing responsibility, and so on. When activities are mediated or implemented by computers, they have new features. The issues have a new twist that make them unusual, even though the core issue is not. For example, before computers, we never had to think through property rights in terms of lines of code that could be implemented by a machine, but throughout history new discoveries have repeatedly challenged traditional notions of property. We have never confronted a threat to privacy of the kind or scale that computers make possible, but other technologies, such as cameras and telephones, have threatened privacy in the past. It is the same when it comes to electronic networks. Activities in networks have special features, though the activities themselves do not fall into new categories of human behavior. We send messages, exchange information, use language, play, work, and so on. With computer networks we have new versions of activities that take place offline and new species of problems that have arisen before.

In this article I identify three special features of online communication and briefly discuss the moral implications of each. I focus on anonymity and uncover its benefits and dangers.

### Special Characteristics of Communication in Networks

Communication in computer networks has several characteristics that make it different from face-to-face communication and other forms of technology-mediated communication, such as telephone, fax, and mass media. These features may make a moral difference in the sense they may make behavior in an electronic network

morally different from offline behavior.

### Scope

Individuals communicating in electronic networks have a much broader reach than they do offline. A message sent by one individual can reach vast numbers of individuals around the world and may do so very quickly. The combination of factors—number of individuals reached, speed, and availability to individuals—makes the scope special. The speed/immediacy of online communication is not unusual in itself, for it is available in face-to-face and telephone communication. Also, the vastness of the reach is not unusual in itself in that radio, television, and telephones have the same reach. With radio and television, however, communication is one way and with telephone communication, it is typically restricted to only two or a few individuals at a given time. Moreover, interactivity is not unusual itself, since it is a given in face-to-face communication. It seems to be the combination of vastness of reach, immediacy, and availability to individuals for interactivity that makes for something unusual here. I use *scope* to refer to all three of these factors together.

We might think of scope as power.

An action—a communication or transfer of information—in a network can have much greater power than an action in ordinary space. When I say something to someone standing next to me or publish an article in a journal, my action has a certain reach which is a function of the physical world. In a network, the impact of a comparable act is magnified many times over. I post an idea to an electronic bulletin board, and it reaches thousands of people around the world in a very short time. Moreover, it may exist, in the sense of being available to others, virtually forever. Similarly, I write some computer code offline, and my action brings about some changes in the way my computer works; I write some computer code online (say, a worm), send it out, and it brings down systems across the world.

One way scope or power has moral implica-

Trust is difficult to develop in an environment in which one cannot be sure of the identities of the people with whom one is communicating.

tions is that we generally expect those engaged in powerful activities to take greater care. We restrict who can use powerful technologies, for example, by licensing their use. We license automobile drivers, pilots, and those who perform surgery, and we regulate many types of businesses that involve dangerous industrial processes. We expect and require those who use more powerful, especially dangerous, technologies to take more precautions and exercise greater care than those who use less powerful technologies, like a megaphone, or a camera. Indeed, we often hold individuals legally liable for the effects of their actions when they use powerful technologies recklessly.

### Anonymity

In networks, individuals can communicate without identity, using pseudonyms and taking on different personas. Moreover, someone may grab someone else's words and alter them or grab someone else's identity and distribute words as if they were the words of the other. In face to face,

telephone, and media communication, individuals can wear disguises and lie about who they are and what they want; voices can be altered through the telephone; reporters can fabri-

cate video material; and FBI agents can go undercover. The distinction is that offline anonymity requires effort on the part of the individual seeking anonymity whereas online, anonymity is often the natural state; at least, it is in those environments where an individual is given a generic user ID. The individual must make an effort in order to establish his or her real identity. In this sense, anonymity may be said to be favored in online communication.<sup>2</sup> Furthermore, the ultimate test of identity offline is seeing the person face to face. The fact that this test is not available online also seems to favor anonymity.<sup>3</sup>

Anonymity creates problems of integrity. The anonymity disconnects the words from the person. It is possible for my words to be taken by someone and distributed as his or her words; for my words to be taken, altered, and then distributed as my words; and for words to be created entirely by someone else and attributed to me. Again, comparable disconnections can and do happen in ordinary space, but they require quite different physical behaviors.

The moral significance of these characteristics will be explored later. For the moment, it is important to note

that trust in the information we use in decision making and trust in the individuals with whom we have relationships seems crucial to our way of being. Yet trust is difficult to develop in an environment in which one cannot be sure of the identities of the people with whom one is communicating. It is difficult to develop a reliable history of experiences with specific people.

### Reproducibility

Information can be reproduced online without loss of value and in such a way that the originator or holder of the information would not notice. Of course, in the ordinary world, information can be reproduced via copying machines and cameras. In electronic networks, however, there is no loss of value in the process of reproduction; a copied program or copied data set is perfectly usable, and the reproduction can be such that there is no evidence that copying has been done—that is, the person who created or owns the information has no reason to believe it has been copied. The difference here is the difference between taking a painting—the painter or owner no longer has the

painting and can see it is gone—and copying a data set—the creator or owner still has the data set and may have no indication a copy was made.

Another aspect of reproducibility is that activities in an electronic network can be recorded and observed. In ordinary space, I utter a sentence to a friend, my friend hears, and understands, and the words are gone (or, at most, retained in the memories of my friend and me). Not so in most forms of online communication. The words are there until someone or some event deletes them. Depending on where I have sent them, they may be available to others who can copy and send them to others ad infinitum, or they may be available to those who manage and monitor the technology, or they may be available to snoopers.

Reproducibility is related to both scope and anonymity. Reproducibility creates the possibility of permanence or, at

**Users must become aware of the meaning and consequences of their actions online.**

<sup>2</sup> It would be a mistake to claim that anonymity is an intrinsic feature of the technology for the technology could be physically designed to diminish the possibility of anonymity.

<sup>3</sup> Screen-image to screen-image contact is available and is likely to improve in quality over time, but it is unlikely this will ever be as credible as seeing a person face to face since screen-image to screen-image contact may lead to virtual-image to virtual-image contact.

least, endurance of information. This adds to the increased scope of actions in networks; that is, actions endure in computer networks. The problem of integrity of information that arises from anonymity (the disconnection between words and person) also arises from the reproducibility of the information. One can anonymously grab words and attribute or alter them because of their reproducibility.

Reproducibility has moral implications because it goes counter to our traditional notions of property and personal privacy. Our notions of property are associated with the idea of control: An owner can control the use of her or his property. Our notions of privacy are based on a physical world in which actions are performed and then are gone; they are irretrievable. (Tape recorders and cameras have also changed this.) In the case of electronic networks, the medium in which an action occurs makes reproduction and observation easier than in ordinary space. Though it depends on how the system is set up, effort is generally necessary to delete an action in a computer network, whereas in ordinary space, effort is necessary to record it. So reproducibility, like anonymity, seems to be favored in computer networks.

In summary, these three special features of communication in networks lead, either directly or indirectly, to problems online.<sup>4</sup> The breadth of scope means that individuals can do a wide variety of things to one another online that would be impossible or extremely difficult to do offline. Individuals can do things to one another online that would require physical closeness and a different set of physical behaviors offline. They can snoop, steal, harass, defame, and sabotage; they can affect thousands of individuals who are vastly geographically distant. Anonymity leads to serious problems for the integrity of information and communication. Reproducibility also threatens the integrity of information, and it means that acts of communication and/or information have endurance. Reproducibility also facilitates surveillance.

## Benefits and Dangers

A wide variety of forums now exist for informal interaction online—different kinds of bulletin boards, discussion groups, email, role-playing games, and so on. All three of the characteristics discussed earlier are likely to be addressed and affected as electronic networks evolve. Each offers benefits and creates dangers.

The benefits and dangers seem to come together. The scope of network communications, for example, brings people together, makes the world seem smaller, and opens up opportunities for increased exchange of ideas and information; at the same time, it brings greater danger of harm on a grander scale. Reproducibility creates the possibility of making massive amounts of information available to many more individuals than ever before, at very little cost, with great convenience, and so on. At the same time,

reproducibility also means greater opportunity for theft and sabotage of information.

Anonymity poses several benefits and dangers. The anonymity available online is likely to figure prominently in the future development of networked communication systems, both as a feature to be preserved and as a feature to be controlled. Clarity on its value and disvalue will ensure that we take advantage of its benefits and minimize its dangers.

Anonymity does not seem to be bad in itself. In fact, it can be beneficial in certain contexts, such as when race, gender, or physical appearance gets in the way of fair treatment. In these contexts, anonymity serves as an equalizer. In online education, for example, biases are removed from student-to-student interactions as well as from the teacher's evaluations of students. Anonymity may also facilitate participation in certain activities. Individuals who might not otherwise participate in discussions with, say, other rape victims or battered wives or ex-criminals may be more willing to take part under the veil of anonymity. Participation may provide individuals with valuable information or much-needed emotional release. Even in less sensitive contexts, individuals may be more likely to say what they think when they have a degree of anonymity. In formal situations, such as in the workplace, individuals may think more creatively and provide better feedback to authorities when they have the veil of anonymity.

Nevertheless, anonymity is problematic in networks, and this seems to be so for at least three related reasons:

- Offline as well as online, anonymity is problematic because it makes the process of identifying and catching criminals more difficult. Here anonymity is still not bad in itself but bad because of the effect it has. Tracking down those who snoop, steal, and sabotage, as well as those who harass or libel others, is made more difficult.
- The second problem with anonymity is related directly to one of its previously mentioned advantages. Anonymity creates a veil under which people are not afraid to say what they think. This is good when it facilitates discussions that are likely to help discussants deal with their feelings, find comfort from those who have had similar experiences, or acquire useful information. On the other hand, anonymity is not so good when it frees individuals to behave in undesirable and

---

<sup>4</sup>We should resist the temptation to think of these characteristics as intrinsic features of computer network communication. In ordinary space, it may seem that privacy is favored because of our bodies and brains. However, we build walls; pass laws specifying that criminal justice agencies cannot wiretap without cause; and expect our neighbors will not aim telescopes at our windows. The same can be said about the special features of computer networks as they have been designed to embody certain characteristics.

harmful ways [6, 9, 12]. Those who might not snoop, steal, harass, make racist comments, or confront others with pornography offline may be more likely to do so under the veil of anonymity online. Being observed and identified by others seems to serve as a form of social control on undesirable behavior, one that is not present online.

- Anonymity contributes to the lack of integrity of online information. We are inundated with information offline and online and thereby forced to make choices about what to rely upon, such as what information to give weight to, when we form opinions and make decisions. One of the ways we do this is by developing a history of experiences with various sources of information. Over the course of time, based on our experiences, we come to trust some sources more than others, or to trust certain sources for certain purposes. This is true in both personal relationships and our relationships with the media. The best example is the way in which individuals typically deal with the wide variety of news sources—newspapers, magazines, and individual reporters. Experiences with each help one to make judgments about which to rely upon for what.

However, this way of dealing with massive amounts of information is not available in an environment in which the identities of the sources of information are uncertain. The same person may be contributing information under multiple identities; the same identity may be used by multiple individuals. In effect, you don't know the sources of the information you receive; you can't develop a history of experiences with a source. The fact that words can be stolen and altered contributes to this problem.

### **Diminished Trust**

These three problems with anonymity contribute to a general situation of diminished trust. One cannot put one's trust in information and individuals online for a variety of reasons: One does not know (at least, in the ordinary sense of "know") the individuals with whom one is communicating. The system of communication is vulnerable to sabotage. Individuals are more likely to behave in undesirable ways when they are anonymous,

so you can't be sure how you will be treated.

The problem of diminished trust comes into focus when we consider the case in which women in an online discussion group on women's issues discovered that a participant whom they believed to be an older single woman confined to a wheelchair was in reality a male psychiatrist in his 30s [10]. The women who participated in the forum were shocked and upset when they found out that a person with whom they shared their intimate thoughts was not who they thought she was. We might view this simply as a case of deception, but that would miss an important component. Participants in the discussion group had come to place their trust in a persona based on a history of experiences (communications) with that persona. I presume they felt betrayed when they discovered the participant's true identity.

Now, some might say the women who participated in the forum were wrong to put any trust in an online persona. They were naive to assume that anyone online is who they claim to be. This response is disturbing, for it suggests that we must give up trust altogether when it comes to online communication. At this point in time it may well be smart to presume very little and to be very cautious. However, it would be a shame if we came to accept diminished trust as a given in online communication. There is no reason to believe that conditions necessary for more trust could not be created.

Trust seems to be built on the development of expectations which continue to be met. Individuals feel deceived and betrayed when their expectations are not met. I expect that my friend will not tell anyone what I have said. I expect when I enter a discussion with colleagues that what I say will be treated with respect. I expect that my friends will not lie to me. And so on. My trust is betrayed when individuals fail to fulfill these expectations.

How expectations are created is an extremely complicated matter. Quite often they are embodied in cultural patterns and institutional structures and transmitted implicitly. Other times they are formally created and meticulously reinforced. Other times they are quite informal. They are generally diverse; that is, individuals have differing expectations about the same situation.

### **Variety and Consent**

What seems most important in promoting trust is that there be some sort of match between what individuals expect and what actually happens. In

this regard, what seems most important for computer networks is that individuals be informed about what to expect when they enter an online environment and that the environment be what it purports to be.

We can have a wide variety of forms of online communication with a high level of trust if the rules are known or explained to individuals before they enter an environment. We can have environments in which there is a high degree of anonymity, environments in which an operator goes to great lengths to check and verify the identity (and even the credentials) of participants before allowing them to participate, and environments between these two extremes. We can have filtered and unfiltered discussions, discussions filtered by diverse criteria. The important thing is that individuals know what they are getting into before they enter.

This approach will not solve all the problems of social behavior online by any means. Indeed, many forms of online discussion are already taking place, and it is clear one of the persistent problems is how to deal with individuals who refuse, for whatever reason, to play by the rules. The important and difficult issues for any individual or group of individuals setting up an informal discussion arena online are deciding how open or closed the forum should be, and how to deal with those who refuse to behave according to the rules.

The primary principle that ought to be followed now is that the rules be specified up front, that is, before a individual begins using a system. Variety can prevail as long as those who communicate online understand the rules of various modes of electronic exchange vary. The metaphor of different rooms works well here. What the rules are depend on where you go. Some rooms are private, some public. Some have narrow purposes and familiar cultures. Others are broad and/or may have strange cultures. But wherever you go, you are either informed immediately or can find out easily what the rules are and what the consequences of violating the rules will be.

## Conclusion

Law and technology will never be enough to solve online behavioral problems. Individuals will have to internalize norms of behavior for their online interactions. After identifying three special features of online communication as compared with offline communication, I have argued that anonymity has benefits and dangers. My analysis suggests we need not insist individuals always be anonymous or always reveal their identities. Rather, I have argued for instituting a principle whereby the rules of all forums are explicit and the consequences for violation are specified. Then individuals can choose which forums they want to join and will know what to expect as they participate.

The ethical issues that arise online are not so different from ethical issues offline. Hence, it should not surprise us

if the most defensible norms for behavior online are identical to norms of behavior offline. Online ethics would seem to call for the following general rules:

1. Know the rules of the forums in which you communicate and follow them.
2. Respect the privacy and property rights of others. When in doubt, assume the user wants privacy and ownership.
3. Respect the individuals with whom you communicate and those who are affected by your communication; that is, do not deceive, defame, or harass. ■

## ACKNOWLEDGMENTS

I am particularly grateful to Chuck Huff for pointing me to the relevant social science literature and to Peter Neumann for his editing.

## REFERENCES

1. Branscomb, A. W. Rogue computer programs and computer rogues: Tailoring the punishment to fit the crime. *Rutgers Comput. Tech. Law J.* 16 (1990), 1–61.
2. Charles, R. Computer bulletin boards and defamation: Who should be liable? Under what standard? *J. Law Tech.* 2 (1987), 121–150.
3. Dibbell, J. A rape in cyberspace. *The Village Voice* 38 (Dec. 21, 1993), 36–42.
4. Gurak, L.J. The rhetorical dynamics of a community protest in cyberspace: The case of Lotus Marketplace. Dissertation, Rensselaer Polytechnic Institute, 1994.
5. Johnson, D.G. *Computer Ethics*. Prentice Hall, Englewood Cliffs, N.J., 1985, 1994.
6. Kiesler, S., Siegel, J. and McGuire, T.W. Social psychological aspects of computer-mediated communication. *Am. Psychol.* 39, 10 (1984), 1123–1134.
7. Levy, S. Battle of the Clipper chip. *NY Times Mag.* (June 12, 1994), 44.
8. Spafford, E. H. Are computer hacker break-ins ethical? In *Computers, Ethics, and Social Values*, D.G. Johnson and H. Nissenbaum, Eds. Prentice-Hall, Englewood Cliffs, N.J., 1995.
9. Sproull, L. and Kiesler, S. Reducing social context cues: Electronic mail in organizational communication. *Manage. Sci.* 32, 11 (Nov. 1986), 1492–1512.
10. Stone, A. R. Will the real body please stand up? In *Cyberspace: First Steps*, M. Benedikt, Ed. MIT Press, Cambridge, Mass., 1991, 81–118.
11. Winner, L. A victory for computer populism. *Tech. Rev.* (May/June, 1991), 66.
12. Zimbardo, P.G. The human choice: Individuation, reason, and order versus deindividuation, impulse, and chaos in Nebraska. In *Symposium on Motivation*, W.J. Arnold and D. Levine, Eds. University of Nebraska Press, Lincoln, 1969.

---

DEBORAH G. JOHNSON ([johnsd@mail1.its.rpi.edu](mailto:johnsd@mail1.its.rpi.edu)) is a professor of philosophy in the Department of Science and Technology Studies at Rensselaer Polytechnic Institute, Troy, N.Y.

---

Permission to make digital/hard copy of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage; the copyright notice, the title of the publication, and its date appear; and notice is given that copying is by permission of ACM, Inc. To copy otherwise, to republish, to post on servers, or to redistribute to lists requires prior specific permission and/or a fee.