Frances S. Grodzinsky and Herman T. Tavani
"Ethical Reflections on Cyberstalking"

Frances S. Grodzinsky is a Professor of Computer Science and Information Technology at Sacred Heart University in Fairfield, CT in the Computer Science/Information Technology department. She is a frequent contributor to computer ethics journals.

Herman T. Tavani is Professor and Chair of the Philosophy Department and Director of the Liberal Studies Program at Rivier College in Nashua, NH. The author of numerous publications in applied ethics, his recent books include Ethics and Technology: Ethical Issues in Information and Communication Technology *(John Wiley & Sons, 2004) and two anthologies co-edited with Richard Spinello:* Readings in CyberEthics *(Jones and Bartlett Publishers, 2004); and* Intellectual Property Rights in a Networked World: Theory and Practice *(forthcoming 2004).*

In this article, Grodzinsky and Tavani examine some ethical aspects of stalking behavior in cyberspace, concentrating on the implications that cyberstalking has for our notion of moral responsibility. They also examine questions about the moral responsibilities of Internet Service Providers.

As You Read, Consider This:

1. What is the difference between cyberstalking and harassment?
2. Who was Amy Boyer? Describe what happened to her.
3. In what ways, if any, does cybertechnology make a moral difference in assessing cases such as Amy Boyer's?
4. What is the Spinello view? How does that contrast with the Vedder view?

Ethics and Information Technology, Vol. 4(2) (2002), pp. 123–132.

1. Introduction: Stalking Incidents in Cyberspace

What is cyberstalking? And how do stalking incidents in cyberspace raise ethical concerns? In answering these questions, we begin with a definition of stalking in general. According to *Webster's New World Dictionary of the American Language*, to engage in stalking is "to pursue or approach game, an enemy, etc. stealthily, as from cover." In the context of criminal activities involving human beings, a stalking crime is generally considered to be one in which an individual ("the stalker") clandestinely tracks the movements of another individual or individuals ("the stalkee[s]"). Cyberstalking can be understood as a form of behavior in which certain types of stalking-related activities, which in the past have occurred in physical space, are extended to the online world. We should note, however, that criteria used in determining which kinds of behavior should count as stalking crimes in the physical realm has been neither consistent nor clear. Hence, it has been even more difficult to determine what the criteria should be for determining a stalking crime in the cyber-realm.

One difficulty in understanding some of the essential features of cyberstalking crimes is that they sometimes border on, and thus become confused with, broader forms of "harassment crimes" in cyberspace. Consider a recent incident involving twenty-year-old Christian Hunold, who was charged with terrorizing Timothy McGillicuddy, a high school principal in the state of Massachusetts. Hunold constructed a Web site that included "hit lists" of teachers and students at that Massachusetts school, on which he also included a picture of the school that was displayed through "the cross hairs of a rifle." Using various pseudonyms, Hunold corresponded with several eighth graders in the school. He then made specific threats to these Massachusetts students, who had no idea that they were communicating with a person who lived in Missouri ("The Web's Dark Side," 2000). Should this particular criminal incident be viewed as a case of cyberstalking? Or is it better understood under a different description such as "cyber-harassment?"

A criminal incident involving Randi Barber and Gary Dellapenta is sometimes also included under the category of cyberstalking. In 1996, Barber met Dellapenta, a security guard, through a friend. Although Dellapenta wanted a relationship with Barber, she spurned his advances. A few months later, Barber began to receive telephone solicitations from men; and in one instance, a "solicitor" actually appeared at the door of her residence. Barber seemed to be unaware of how potentially dangerous her situation had become. For example, she had no idea that Dellapenta had assumed her identity in various Internet chat rooms, when soliciting "kinky sex." Anonymity and pseudonymity tools, available to any Internet user, allowed Dellapenta to represent himself as Barber, via screen names such as a "playfulkitty4U" and "kinkygal30." Barber became aware of what was going on only after she asked one caller why he was phoning her (Foote, 1999). Note that in this alleged case of *cyber*stalking, Dellapenta engaged others to "stalk" his intended victim in physical space. So once again, we can ask whether the Barber/Dellapenta incident is a genuine case of cyberstalking or whether it can be more appropriately described as instance of a harassment involving the use of Internet technology.

Thus far we have briefly described two different criminal incidents that some authors have referred to as examples of cyberstalking. It is perhaps worth noting that no physical harm resulted to victims in either incident; and in both cases, it was difficult to separate certain harassment activities (in general) from stalking behavior in particular. Also, in the Barber/Dellapenta case, the stalking-related activities involved both physical space and cyberspace. We next examine a stalking incident involving Amy Boyer, which we believe is a clearer case of cyberstalking.

2. The Amy Boyer Cyberstalking Case

On October 15, 1999, Amy Boyer, a twenty-year-old resident of Nashua, NH, was murdered by a young man who had stalked her via the Internet. Her stalker, Liam Youens, was able to carry out most of the stalking activities that eventually led to Boyer's death by using a variety of online tools available to any Internet user. Through the use of online search facilities, for example, Youens was able to find out where Boyer lived, where she worked, what kind of vehicle she drove, and so forth. Youens was also able to use other kinds of online tools, typically provided by Internet service providers (ISPs), to construct two Web sites. On one site, he posted personal information about Boyer, including a picture of her; and on another site, Youens described, in explicit detail, his plans to murder Boyer.

The Amy Boyer case raises several ethical and social questions, independent of the important fact that the stalking behavior in this incident eventually led to Boyer's death. For example, some have argued that Boyer's privacy was violated. We could ask whether Boyer was the victim of online defamation. We could also ask whether Youens had a right to post information about Boyer on his Web site, and whether such a "right" is one that ought to be protected by free speech. Or should such "speech" be controlled in cyberspace? Also, we could ask whether issues raised in the Boyer case are more ethically significant than those in other online stalking incidents because of the physical harm caused to Boyer resulting in her death. Although the Amy Boyer case raises several ethical issues, we can ask whether there is anything unique or even special about these issues from a moral point of view.

3. What, if Anything, Is Ethically Significant about Cyberstalking Crimes?

From an ethical perspective, an interesting question is whether there is anything unique or even special about the Amy Boyer case in particular, or cyberstalking in general. On the one hand, we do not claim that cyberstalking is a new kind of crime; nor, for that matter, do we argue that cyberstalking is a "genuine" computer crime" (Tavani, 2000). Yet we can reasonably ask whether Internet technology has made a relevant difference in the stalking case involving Amy Boyer. Perhaps the more important question, however, is: Has cybertechnology made a moral difference? One might be inclined to answer *no*. For example, one could argue that "murder is murder," and that whether a murderer uses a computing device that included Internet tools to assist in carrying out a particular murder is irrelevant from an ethical point of view. One could further argue that there is nothing special about cyberstalking incidents in general—irrespective of whether or not those incidents result in the death of the victims—since stalking activities have had a long history of occurrence in the "off-line" world. According to this line of reasoning, the use of Internet technology could be seen as simply the latest in a series of tools or techniques that have become available to stalkers to assist them in carrying out their criminal activities.

However, it could also be argued that the Internet has made a relevant difference with respect to stalking-related crimes because of the ways in which stalking activities can now be carried out. For example, Internet stalkers can operate anonymously or pseudononymously while online. Also consider that a cyberstalker can stalk one or more individuals from the comfort of his or her home, and thus does not have to venture out into the physical world to stalk someone. So Internet technology

has provided stalkers with a certain mode of stalking that was not possible in the pre-Internet era (Tavani, 2002).

It could also be argued that cyberstalking has made possible certain kinds of behavior that challenge our conventional moral and legal frameworks. These challenges have to do primarily with issues of *scale* and *scope*. For example, a cyberstalker can stalk multiple victims simultaneously through the use of multiple "windows" on his or her computer. The stalker can also stalk victims who happen to live in states and countries that are geographically distant from the stalker. So, potentially, both the number of stalking incidents and the range of stalking activities can increase dramatically because of the Internet. However, we leave open the question of whether any of these matters make a moral difference.

In the remainder of this essay, we focus on two questions involving issues of moral responsibility in the Boyer case: (1) Should the two ISPs that permitted Youens to post information about Amy Boyer on Web sites that reside in their Internet "space" be held morally accountable? (2) Do ordinary users who happen to come across a Web site that contains a posting of a death threat directed at an individual (or group of individuals) have a moral responsibility to inform those individuals whose lives are threatened?

4. Moral Responsibility and Internet Service Providers (ISPs)

As noted above, Youens set up two Web sites about Amy Boyer: one containing descriptive information about Boyer, as well as a photograph of her, and another on which he described in detail his plans to murder Boyer. To what extent, if any—either legally or morally, or both—should the ISPs that hosted the Web sites created by Youens be held responsible? Because this question is very complex, it would be beneficial to break it down into several shorter questions. For example, we first need to understand what is meant by "responsibility" in both its legal and moral senses. We also have to consider whether we can attribute moral blame (or praise) to an organization or collectivity (i.e., a group of individuals), such as an ISP. We begin by briefly examining some recent laws and court challenges that either directly or indirectly pertain to questions involving responsibility and liability for ISPs.

In *Stratton Oakmont v. Prodigy Services Company* (1995), the court determined that Prodigy could be held legally liable since it had advertised that it had "editorial control" over the content in the computer bulletin board system (BBS) it hosted. In the eyes of the court, Prodigy's claim to have editorial control over its BBS made that ISP seem similar to a newspaper, in which case the standard of strict legal liability used for original publishers could be applied. In response to the decision in the Prodigy case, many ISPs have since argued that they should not be understood as "original publishers," but rather as "common carriers," similar in relevant respects to telephone companies. Their argument for this view rested in part on the notion that ISPs provide the "conduits for communication but not the content." This view of ISPs would be used in later court decisions (such as *Zeran v. America Online Inc.* 1997).

In Section 230 of the Communications Decency Act (CDA), the function of ISPs was interpreted in such a way that would appear to protect them from lawsuits similar to the one filed against Prodigy. Here the court specifically stated, "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." Although the U.S. Supreme Court eventually struck down CDA, Section 230 of that Act has remained intact. While ISPs are not legally liable for the content of their Web sites or for the

content of other electronic forums that they also might host—e.g., forums such as bulletin boards, chat rooms, and list servers—they have nonetheless been encouraged to monitor and filter, to the extent that they can, the content of these electronic forums. But this has presented ISPs with a thorny legal problem. Consider, for example, that the more an ISP edits content, the more it becomes like a publisher (such as a newspaper). And the more it becomes like a publisher, with editorial control, the more liable an ISP becomes from a legal perspective. So, effectively, there could be some disincentive for ISPs to monitor and filter content. This, in turn, raises a moral dilemma for ISPs.

Should Internet Service Providers be held morally accountable for objectionable behavior that occurs in their forums? Deborah Johnson (2001) notes that while it might be easier to make a utilitarian case for holding ISPs legally liable in certain instances, it would be much more difficult to make the case that ISPs should be morally responsible for the behavior of their customers. Recently, however, Richard Spinello (2001) and Anton Vedder (2001) have tried to show, via different very different kinds of arguments, why ISPs also should be held morally accountable to some extent. Neither Spinello nor Vedder address the issue of cyberstalking per se; however, we believe that Spinello's remarks regarding "on-line defamation" and Vedders's comments regarding on-line "harm," both of which are associated with ISPs, can help shed some light on the question before us. We briefly examine both arguments.

4.1 The Spinello View

Arguing that ISPs should be held morally accountable in cases involving defamation, Spinello first distinguishes between "moral responsibility" and "moral accountability." In making this distinction, he uses a model advanced by Helen Nissenbaum (1994). According to Nissenbaum's scheme, accountability, unlike responsibility, does not require *causality* or a causal connection. Spinello points out that because ISPs do not *cause* defamation, they cannot be held responsible in the strict or narrow sense of the term. However, he argues that they could, nonetheless, be held accountable—i.e., "answerable"—in the sense that they "provide an occasion or forum" for defamation. Spinello is careful to point out that simply because an ISP presents an "occasion for defamation," it does not necessarily follow that an ISP is accountable. Rather, for an ISP to be accountable, two further conditions are required: (a) the ISP must also have some *capability* to do something about the defamation, and (b) the ISP failed to take action once it had been informed. Spinello believes that this standard of accountability takes into consideration what ISPs can reasonably do—i.e., what they are *capable* of doing—to prevent defamation or at least to limit its damage. So the fact that an ISP might not have caused the defamation does not rule out the possibility that the ISP can be held accountable in some sense for defamatory remarks.

Spinello concedes that technical and economic factors make it virtually impossible for ISPs to take preventative, or what he calls "pre-screening," measures that would detect or filter out defamatory messages. Thus we cannot hold ISPs responsible in a causal sense for defamation. Assuming that Spinello's overall argument is correct, however, we might hold ISPs accountable if they fail to take certain actions once they are informed that a victim has been defamed. For Spinello, these steps would include three actions: (i) prompt removal of the defamatory remarks; (ii) the issuance of a retraction on behalf of the victim; and (iii) the initiation of a good faith effort to track down the originator so that the defamation does not reoccur.

Does this threefold requirement provide us with a standard of accountability that is a "reasonable middle ground," as Spinello suggests? Or is it an unreasonable expectation for ISPs? Spinello

notes that in the current system, a victim of defamation has no legal recourse because of the absolute immunity given to ISPs. On the other hand, the strict legal liability that was applied in the Prodigy case seems unduly harsh for ISPs. So Spinello believes that his alternative scheme provides the appropriate middle ground needed, because it grants some protection to victims of defamation without burdening the ISP. So even if the law does not require ISPs to take any action, Spinello believes that "post-screening" in a "diligent fashion" for content along the lines of the threefold criteria described above is the morally right thing to do. He concedes, however, that ISPs do not have the capability to "pre-screen" content for defamation.

4.2 The Vedder Argument

Anton Vedder (2001) has recently advanced a very different kind of argument for why we should consider holding ISPs morally responsible for harm caused to individuals. Vedder suggests that we begin by drawing an important distinction between two senses of moral responsibility: *prospective* and *retrospective* responsibility. Whereas retrospective responsibility tends to be "backward looking," prospective responsibility is "forward looking." Vedder believes that in the past, arguments that have been used to ascribe legal liability to ISPs have tended to be prospective in nature. This is because the primary objective of liability laws has been to deter future on-line abuses rather than punish past offenses.

Vedder also notes that even though ISPs are not legally liable for their content under current US law, the mere threat of legal liability can be used to deter ISPs from becoming lax about "policing" their electronic forums to some reasonable extent. So underlying the reasoning for arguments for applying strict legal liability to ISPs is the utilitarian principle that having liability laws in place will deter harm to ISP users in the future. And this legal argument, in turn, is based on a notion of moral responsibility that is essentially *prospective* in nature. Vedder also points out that we are hesitant to attribute a retrospective sense of responsibility to ISPs because this sense of moral responsibility:

(a) is usually applied to individuals (as opposed to organizations or what he calls "collectivities"), and
(b) it also often implies guilt.

And as Vedder correctly notes, the notion of guilt is typically attributed to individuals and not to organizations or collectivities. He suggests, however, that in some cases it also makes sense to attribute the notion of guilt to a collectivity such as an ISP.

Attributing some moral accountability to ISPs makes sense, in Vedder's scheme, because of the connection that exists between retrospective and prospective responsibility. Vedder argues that it makes no sense to hold an agent (i.e., either an individual or a collectivity) responsible for an act in a prospective sense if that agent could not also be held responsible for the act in a retrospective sense as well. So Vedder concludes that if we assume that collectivities such as ISPs can be held responsible in a prospective sense—a rationale that has been used as the basis for utilitarian arguments in attributing legal liability for ISPs—then we can also ascribe retrospective responsibility to ISPs. So, as in the case of Spinello, Vedder believes that ISPs can be held morally accountable to some extent for speech that is communicated in their electronic forums.

4.3 Implications for the Amy Boyer Case

We can now apply Vedder's and Spinello's arguments to the Amy Boyer cyberstalking case. Should Tripod and Geocities, the two ISPs that enabled Liam Youens to set up his Web sites about Boyer, be held morally accountable for the harm caused to Boyer and to her family? And should those two ISPs be held morally accountable, even if they were not responsible (in the narrow sense) for causing harm to Boyer and even if they can be exonerated from charges of strict legal liability? If the arguments by Vedder and Spinello succeed, then it is reasonable to hold these ISPs morally accountable if it also could be shown that Tripod and Geocities were capable of limiting the harm that resulted to Boyer. (Tim Remsberg, Amy Boyer's stepfather, has recently filed a wrongful death suit against both ISPs.)

Of course, one might ask what the purpose would be in attributing moral responsibility to ISPs if no legal action could be taken against them. At least two different replies are possible to this question, both of which might also cause us to be more careful in our thinking about moral issues involving cyberspace. First, an analysis of moral issues in this light could help us to distinguish further between moral and legal aspects of controversial cyberspace issues. Second, such an analysis can also help to consider some ways in which moral responsibility can be applied at the collective, as well as at the individual, level.

5. Individual Moral Responsibility at the Level of Ordinary Internet Users

We next examine questions of moral responsibility that apply at the individual level, i.e., at the level of individual users in online communities. For example, do ordinary Internet users have a moral responsibility to inform "would-be victims" of their imminent danger to online stalkers? If an Internet user had been aware of Boyer's situation, should that user have notified Boyer that she was being stalked? In other words, should that user be morally obligated to do so?

Various proposals for controlling individual behavior in online communities have resulted in a conflict between those who wish to regulate strictly by law and those who wish to preserve the practice of self-regulation. Of course, this dispute is sometimes also at the base of arguments involving claims having to do with a "safe" social space vs. a "restrictive" one. In the case of cyberstalking, should we assist others based strictly on formal legal regulations, or should we assist them because it is the morally right thing to do?

5.1 A Minimalist Sense of Moral Obligation vs. an "Ethic of Care"

Some have argued that while morality can demand of an agent that he or she "do no harm" to others, it cannot *require* that an agent actively "prevent harm," or "do good." In one sense, to do no harm is to act in accordance with the rules of a moral system. But is doing so always sufficient for complying with what is required of us as moral agents? In other words, if it is in our power to prevent harm and to do good, should we do so? Some theoretical frameworks suggest that individuals should prevent harm (and otherwise do good) whenever it is in their power to do so. For example, if one believes, as some natural law theorists assert, that the purpose of morality is to alleviate human suffering and to promote human flourishing, whenever possible, then clearly we would seem obligated to prevent harm in cyberspace. An interesting account of this view has been advanced by Louis Pojman (2001).

Unfortunately, we are not able to present Pojman's argument here in the detail that it deserves, since doing so would take us beyond the scope of this paper. But we can see how, based on a model like Pojman's, one might develop a fuller theory in which individuals have an obligation to "assist" others in the act of preventing harm from coming to those persons.

We recognize the difficulties of defending a natural law theory; and we are not prepared to do so here. However, we also believe that the kind of limited or "moderate" natural law theories that can be found in Pojman, and to some extent in James Moor (1998), can be very useful in making the case for an extended sense of moral obligation at the level of individuals.

Another moral framework that implies an expanded sense of moral responsibility on the part of individuals is the "ethic of care," introduced in a seminal work by Carol Gilligan (1982). Complying with a "care ethic," individuals would assist one another whenever it is in their power to do so. As such, an ethic based on care is more robust than a mere "non-interference" notion of ethics that simply involves "doing no harm to others"—i.e., it is concerned with a sense of commitment to others that Virginia Held (1995) describes as "above and beyond the floor of duty."

Gilligan's ethic of care has been contrasted with traditional ethical systems, such as utilitarian and Kantian theories. Alison Adam (2000) points out that traditional ethical theories are often based simply on following formal rules and that they tend to engender a sense of individualism (as opposed to community). Adam (2001, 2002) has also argued that an ethic of care, in particular, and feminist ethical theory in general, can help us to understand more clearly some of the social and ethical implications of cyberstalking behavior in ways that traditional ethical theories cannot.

Adopting an "ethic of care" in cyberspace would mean that individuals, i.e., ordinary Internet users, would be prone to assist others whenever they can help to prevent harm from coming to them. From this perspective, individuals would assist one another, even though there may be no specific laws or rules that require them to do so. In what sense would such an expectation on the part of individuals expand our conventional notion of moral obligation?

5.2 Expanding the Sphere of Moral Responsibility: A *Duty to Assist*

Questions concerning whether individuals have a "duty to assist" others often arise in the aftermath of highly publicized crimes such as the one involving in the Kitty Genovese case in 1964. Genovese, a young woman, was murdered on the street outside her apartment building in Queens, New York, as thirty-eight of her neighbors watched. None of her neighbors called the police during the 35-minute period of repeated stabbings. Some have since referred to this refusal to assist a neighbor in critical need as "the Genovese Syndrome." Police involved in the Genovese case believe that the witnesses were morally obligated to notify the police, even though there may have been no formal law or specific statute requiring them to do so.

Drawing an analogy between the Genovese and Boyer cases, we can ask whether users who might have been able to assist Boyer should have done so (i.e., whether they were morally obligated to assist her). We can also ask what kind of community cyberspace will become, if people refuse to assist users who may be at risk to predators and murderers. First, we need to consider the potential harm that could come to members of the online community if we fail to act to prevent harm from coming to those individuals, when it is in our power to help and when doing so would neither cause us any great inconvenience nor put our safety at risk. What would have happened to Randi Barber if no one had intervened in her behalf? In the cyberstalking case involving Barber and Dellapenta,

Barber's father, with the cooperation of the men who were soliciting her, provided evidence that led to Dellapenta's arrest. In the case of Amy Boyer, however, the same sense of individual moral responsibility and concern was not apparent. Consider that some Internet users had, in fact, viewed the Youens Web site but did not inform Boyer that she was being stalked and that her life was in imminent danger. Like Kitty Genovese, who received no assistance from members of her physical community, Amy Boyer received no assistance from members of the online community.

Because of what happened to Amy Boyer, and because of what could happen to future victims of online stalking, we argue that ordinary users, as members of an online community, should adopt a notion of moral responsibility that involves assisting fellow users. Doing so would help to keep cyberspace a safer place for everyone, but especially for women and children who are particularly vulnerable to stalking activities. Failing to embrace such a notion of moral responsibility, on the other hand, could result in users disconnecting themselves from their responsibilities towards fellow human beings.

6. Conclusion

We have examined some ethical concerns involving cyberstalking in general, and the Amy Boyer case in particular. We saw that stalking activities in cyberspace raise questions about the sphere of moral responsibility, both for ISPs and ordinary Internet users. We argued that ISPs and individual users, each in different ways, should assume a more robust sense of moral responsibility, which goes beyond a mere "non-interference ethic," in order to help to prevent harm from coming to individuals targeted by cyberstalkers.

Acknowledgments

We are grateful to Anton Vedder for some very helpful comments on an earlier version of this paper. We also wish to thank Detective Sergeant Frank Paison of the Nashua, NH Police Department, who was the chief investigator in the Amy Boyer cyberstalking case, for some helpful information that he provided during an interview with him.

Portions of this essay are extracted from Tavani (2004). We are grateful to John Wiley & Sons, Publishers for permission to reprint that material.

References

Adam, Alison (2000). "Gender and Computer Ethics." *Computers and Society,* Vol. 30, No. 4, pp. 17–24.

Adam, Alison (2001). "Cyberstalking: Gender and Computer Ethics." In Eileen Green and Alison Adam, eds. *Virtual Gender: Technology, Consumption, and Identity.* London: Routledge, pp. 209–234.

Adam, Alison (2002). "Cyberstalking and Internet Pornography: Gender and the Gaze." *Ethics and Information Technology,* Vol. 4, No. 2, pp. 133–142.

Foote, D. (1999). "You Could Get Raped," *Newsweek,* Vol. 133, No. 6, Feb. 8, pp. 64–65.

Gilligan, Carol (1982). *In a Different Voice.* Cambridge: Harvard University Press.

Grodzinsky, Frances S., and Herman T. Tavani (2001). "Is cyberstalking a Special Type of Computer crime?" In Terrell Ward Bynum, et al., eds, *Proceedings of ETHICPMP 2001: The Fifth International Conference on the Social and Ethical Impacts of Information and Communication Technology.* Vol. 2. Gdansk, Poland: Wydawnicktwo Mikom Publishers, pp.72–81.

Grodzinsky, Frances S., and Herman T. Tavani (2002). "Cyberstalking, Moral Responsibility, and Legal Liability Issues for Internet Service Providers." In Joseph Herkert, ed. *Proceedings of ISTAS 2002: The International Symposium on Technology and Society.* Los Alamitos, CA: IEEE Computer Society Press, pp. 331–339.

Held, Virginia (1995). "The Meshing of Care and Justice," *Hypatia,* University of Indiana Press, Spring.

Johnson, Deborah G. (2001). *Computer Ethics.* 3rd. ed. Upper Saddle River, NJ: Prentice Hall.

Moor, James H. (1998). "Reason, Relativity, and Responsibility in Computer Ethics." *Computers and Society,* Vol. 28, No. 1, 1998, pp. 14–21.

Nissenbaum, Helen (1994). "Computing and Accountability," *Communications of the ACM,* Vol. 37, No. 1, pp. 73–80.

Pojman, Louis P. (2001). *Ethics: Discovering Right and Wrong.* 4th ed. Belmont, CA: Wadsworth.

Spinello, Richard A. (2001). "Internet Service Providers and Defamation: New Standards of Liability." In R. A. Spinello and H. T. Tavani, eds. *Readings in CyberEthics.* Sudbury, MA: Jones and Bartlett, pp. 198–209.

Tavani, Herman T. (2000). "Defining the Boundaries of Computer Crime: Piracy, Break-ins and Sabotage in Cyberspace." *Computers and Society,* Vol. 30, No. 4, 2000, pp. 3–9.

Tavani, Herman T. (2002). "The Uniqueness Debate in Computer Ethics: What Exactly Is at Issue, and Why Does it Matter?" *Ethics and Information Technology,* Vol. 4, No. 1, pp. 37–54.

Tavani, Herman T. (2004). *Ethics and Technology: Ethical Issues in an Age of Information and Communication Technology.* New York: John Wiley and Sons.

Tavani, Herman T., and Frances S. Grodzinsky (2002). "Cyberstalking, Personal Privacy, and Moral Responsibility," *Ethics and Information Technology,* Vol. 4, No. 2, pp. 123–132.

"The Web's Dark Side: In the Shadows of Cyberspace, an Ordinary Week is a Frightening Time," *U.S. News & World Report,* Vol. 129, No. 8, Aug. 28, 2000.

Vedder, Anton H. (2001). "Accountability of Internet Access and Service Providers: Strict Liability Entering Ethics." *Ethics and Information Technology,* Vol. 3, No. 1, pp. 67–74.

Journal/Discussion Questions

1. Have you known anyone who was the object of cyberstalking? What special dimensions were present because the incident occurred in cyberspace?
2. Cyberstalking is only one of several questionable things that happen in cyberspace. What do you think the responsibilities of Internet Service Providers should be in this regard?