3-2002

Some Ethical Reflections on Cyberstalking

Frances Grodzinsky
Sacred Heart University, grodzinskyf@sacredheart.edu

Herman T. Tavani
Rivier College

Recommended Citation

Grodzinsky, Frances, Tavani, Herman T. "Some Ethical Reflections on Cyberstalking." ACM SIGCAS Computers and Society 32.1 (2002): 22-32.

Some Ethical Reflections on Cyberstalking

Frances S. Grodzinsky
Sacred Heart University
<grodzinskyf@sacredheart.edu>

Herman T. Tavani
Rivier College
<htavani@rivier.edu>

Abstract

The present study examines a range of moral issues associated with recent cyberstalking cases. Particular attention is centered on the Amy Boyer/ Liam Youens case of cyberstalking, which raises a host of considerations that we believe have a significant impact for ethical behavior on the Internet. Among the questions we consider are those having to do with personal privacy and the use of certain kinds of Internet search facilities to stalk individuals in cyberspace. Also considered are questions having to do with legal liability and (possible) moral responsibility that Internet Service Providers (ISPs) have for stalking crimes that occur in their "space" on the Internet. Finally, we examine issues of moral responsibility for individual online users to determine which obligations, if any, they might have to inform persons who are targeted by cyberstalkers, when it is in their power to do so.

Keywords

Cyberstalking, personal privacy, search engines, ISPs, moral responsibility, and duty to assist

1. INTRODUCTION: STALKING ACTIVITIES IN CYBERSPACE

What exactly is cyberstalking, and how exactly do stalking incidents in cyberspace raise concerns for ethics? In answering these questions, we begin with a definition of stalking in general. According to *Webster's New World Dictionary of the American Language*, one definition of stalking is "to pursue or approach game, an enemy, etc. stealthily, as from cover." In an extended sense of stalking, as applied to criminal activities involving human beings, a "stalking activity" has come to be associated with one individual ("the stalker") clandestinely tracking the movement and whereabouts of an 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. On the one hand, we do not wish to claim that cyberstalking is a new kind of crime or that it is a "genuine computer crime" (see Tavani, 2000). On the other hand, we believe that the Internet has made a relevant difference because of the way stalking activities can now be carried out (see Grodzinsky and Tavani, 2001). For example, Internet stalkers can operate anonymously or pseudononymously while online. In addition, a cyberstalker can stalk one or more individuals from the comfort of his living room, and thus not have to venture out into the physical world to carry out his task. So Internet technology has made possible certain modes of stalking that would not have been possible in the pre-Internet era.

Many people are concerned about the kind and the number of stalking-related activities that now occur in cyberspace. There are many reasons why these individuals would seem justified in their concern. Because stalking crimes are not fully understood in terms of their conceptual boundaries and their implications, it is that much more difficult to understand clearly what it would mean to stalk someone in cyberspace. In the cyber-realm, for example, there are no physical-space criteria that are strictly analogous to those in physical space.

One difficulty in understanding some of the essential features of cyberstalking crimes is that these crimes sometimes border on, and thus become confused with, broader forms of "harassment crimes." Consider a recent incident involving twenty-year old Christian Hunold, who was charged with terrorizing Timothy

McGillicuddy, principal of a high school in the US. Hunold constructed a Web site that included "hit lists" of teachers and students at the school, and a picture of the school that was displayed through "the cross hairs of a rifle". On that site, Hunold, under various pseudonyms, corresponded with 40 of the 215 eighth graders in the school. He then began to make threats to the victims in Massachusetts who did not know that they were actually dealing with a person who lived in Missouri ("The Web's Dark Side", 2000). Is this behavior a form of cyberstalking or is it "harassment in cyberspace?"

The case of Randi Barber and Gary Dellapenta illustrates an incident in which the stalker himself engaged others to stalk the intended victim in physical space. 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 phone solicitations from men on her telephone answering machine; and in one case, a "solicitor" actually appeared at the door of her residence. Because she had never used a computer or had never interacted with the Internet, Barber had no idea how potentially dangerous her situation was. For example, Barber was not aware that Dellapenta had actually 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". His access to chat rooms and message boards enabled him to disseminate information about Barber to Internet users around the globe. Barber became aware of what was going on only after she asked one caller why he was phoning her. The caller's answer both shocked and frightened her. Barber's anonymous cyberstalker had managed to unleash a chain of threatening events with a few clicks of a mouse (Foote, 1999). Again, we can ask whether the Barber/Dellapenta case is truly cyberstalking instead of a more general instance of harassment

Thus far we have described some particular cases that have been described as cyberstalking activities. We have also seen why, in these particular cases, it was difficult to separate out certain harassment activities (in general) from stalking behavior in particular. In the next section we focus our attention on a specific case of Internet stalking involving Amy Boyer. We will see why this particular case would seem to be a clear instance of cyberstalking. We will also see why the Amy Boyer case raises a range of ethical issues that are philosophically interesting.

2. THE AMY BOYER CASE: SOME ETHICAL IMPLICATIONS

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. The 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 tools available to him online. Through the use of standard Internet search facilities, for example, Youens gathered information about Boyer that was readily accessible from databases available to online search requests. A series of Internet searches on the name "Amy Boyer" yielded several pieces of information about Boyer, which Youens could then piece together to track down his victim. Through the use of certain tools available to any Internet user, he was able to find out where Boyer lived, where she worked, what kind of vehicle she drove, etc. In addition to using Internet search-related tools to acquire personal information about Boyer, Youens was also able to use other kinds of online tools, provided by Internet Service Providers (ISPs), to construct two Web sites. On one site, he posted personal information about Boyer, including her picture, and on another the other site he described, in explicit detail, his plans to murder Boyer.

The Amy Boyer case has raised a number of controversial questions, many of which would seem to have significant moral implications for cyberspace. One question at issue here is whether there really is anything special about Boyer's murder, including the stalking activities that led to her eventual death. In response to the Boyer incident, philosophers taking a position that Deborah Johnson (2001) describes as the "traditionalist" view might argue that there is nothing philosophically or morally interesting about cyberstalking in general, or the Amy Boyer case in particular. A traditionalist would point out, for example, that "murder is murder," and that, unfortunately, several homicides occur each day. On this view, whether a murderer uses a computing device that included Internet tools to assist in carrying out a particular murder would seem irrelevant; or at least it would not intuitively seem to be a factor that makes a qualitative difference in the carrying out of a crime such as homicide. A traditionalist might also take the position 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 "offline" world. On this view, 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.

Those philosophers who could be described as "uniqueness advocates" (see Tavani, 2001) with respect to computer ethics issues, on the other hand, would likely suggest that there are certain aspects of cyberstalking that raise either new or special ethical problems. Proponents of this view can point to a number of factors which, either individually or in combination, would support such a position. For one thing, they can point out the relative ease with which stalking activities can now be carried out in cyberspace. By simply using a computing device with Internet access, one can now stalk a targeted victim without having to leave the comfort of his or her home. Uniqueness advocates could then go on to point to issues having to do with the *scope* of stalking crimes that are now possible. Through the use of Internet technology, for example, an individual can stalk multiple victims simultaneously through the use of multiple "windows" on his computer. The stalker can also stalk victims who happen to live in states and countries that are geographically distant from the stalker. Also, through the use of Internet technology a stalker can, as Liam Youens did, easily acquire personal information about his or her victim because of the availability of such information that is readily accessible from electronic databases via online search engines.

Uniqueness advocates can also point to issues having to do with the aspects of stalking having to do with the *scale* or number of stalking crimes now made possible by cyber-technology. For example, a stalker can roam the Internet anonymously, or under a certain alias (pseudonym), which makes it much more difficult for law-enforcement agents to track down that stalker, either before or after the stalker has caused physical harm to his victim. Because of the ease of electronic stalking, individuals who might never have considered stalking a victim in physical space might be tempted to engage in one or more stalking activities in virtual space. These and other factors, it could be further argued, contribute to the possibility of stalking crimes occurring on a scale that would not likely have been possible prior to the advent of the Internet. It has also been argued that cyberstalking activities have significant implications for a range of ethical and social issues, ranging from those of privacy and security, free speech and censorship to more general questions involving moral responsibility and legal liability (see Grodzinsky and Tavani, 2001).

As mentioned above, our specific concern in this section of the paper is with the stalking incident involving Amy Boyer and with particular ethical questions that the case raises. For example, was Boyer's right to (or at least her expectations about) privacy violated because of the personal information about her that was made available so easily to Internet users such as Liam Youens? Did Youens have a "right" to set up a dedicated Web site about Amy Boyer without Boyer's knowledge and express consent; and did Youens have a right to post on that Web site any kind of information about Boyer — regardless of whether that information about her was psychologically harmful, offensive, or defamatory? If so, is such a right one that is — or ought to be — protected by free speech? Should the two ISPs that enabled Youens to post such information to Web sites that reside in their Internet "space" be held legally liable, especially when information contained on those sites can easily lead to someone 's being physically harmed or, as in the case of Amy Boyer, murdered? Furthermore, 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? These kinds of questions are among those which suggest that there may indeed be something special about the Amy Boyer case (as well as for cyberstalking activities in general) that are worthy of further examination from a moral point of analysis.

Although each of the issues briefly described in the preceding paragraph have significant ethical implications, and while each might deserve deeper philosophical analysis, we will limit our discussion in this section of our paper to three ethical concerns involving the Amy Boyer case. First, we consider the issue of threats posed to potential cyberstalking victims because of the unrestricted use of Internet search engines. We then consider questions of legal liability and moral responsibility in cyberstalking incidents for Internet Service Providers (ISPs). Finally, we consider the role of individual moral responsibility for Internet users who find themselves in a position to inform a fellow user that she is being stalked.

3. INTERNET SEARCH ENGINES AND PUBLIC RECORDS: IMPLICATIONS FOR PERSONAL PRIVACY

Few would dispute the value that Internet search engines have provided in directing us to a host of available online resources, which in turn have aided us locating useful information involving academic research, commerce, recreation, and so forth. Hence, some might be surprised to find that search-engine technology itself could be controversial in some way. However, search engines can also be used to locate personal information about individuals. Sometimes that personal information resides in the form of public records that are available to Internet users, as in the case of information acquired about Amy Boyer by Liam Youens. Other types of personal information about individuals can also be acquired easily because of certain kinds of personal data that has been made accessible to Internet search engines without the knowledge and consent of the person or persons affected. But one might still ask why exactly the use of search-engine technology is controversial with respect to the privacy of individuals. Because an individual may be unaware that his or her name is among those included in one or more databases accessible to search engines, individuals have little control over how information about them can be made available and be disseminated across the Internet (see Tavani, 1997). This was certainly the case in the incident involving Amy Boyer, who had no knowledge about or control over the ways in which certain kinds of personal information about her was accessible to Youens through Internet search engines — for Boyer neither placed any personal information about herself on the Internet, nor was she aware that such information about her had been so placed.

It could be argued that all information currently available on the Internet, including information about individual persons such as Amy Boyer, is, by virtue of the fact that it resides on the Internet, public information. We can, of course, question whether all of the information currently available on the Internet *should* be viewed as public information. And, if the answer to that question is "yes," then should certain kinds of "public information," viz., public records that contain personal information, be treated merely as public data or as data that might deserve some kind of normative protection?

Because of concerns related to the easy flow of personal information between and across databases, certain laws have been enacted and some policies established to set limits on the ways in which electronic records containing *confidential* or *intimate* data can be exchanged. However, these laws and policies typically apply only to the exchange of electronic information such as that contained in medical records and financial records. Helen Nissenbaum (1998) has pointed out that such protection does not apply to personal information in the public sphere or in what she describes as "spheres other than the intimate." Unfortunately for Amy Boyer, the kind of information that was gathered about her by Youens would be considered non-intimate and non-confidential in nature and thus would likely be viewed, by default, as "public" in nature. Is this presumption about how personal information involving public records is currently viewed one that it is either reasonable or fair? Was it fair to Amy Boyer?

What exactly should the status of personal information that resides in public records that now are accessible to everyone be with respect to privacy policies and laws? In particular, what should the privacy status of this kind of information be in the Internet age? It could be noted that in the era preceding the Internet, information of this particular kind could have been acquired by individuals willing to go to certain municipal buildings to request hardcopy versions of public records that contained personal information about various individuals. Of course, individuals requesting such information would have had to physically travel to the municipal building where the information they desired was housed, and those individuals would have probably been charged a small fee for any records they obtained. If this kind of information about persons was already public before the advent of cyber-technology, why should its status necessarily change because of the new technology? Perhaps an equally important question that could be asked as an alternative to the original question is: Why were such records made public in the first place? For example, were they made public so that online entrepreneurs like Docusearch.com could collect this information, combine it with other kinds of personal information, and then sell it for a profit? Of course, it could be argued that entrepreneurs who were so motivated could have engaged in this activity — and some, no doubt, did — in the era preceding the Internet. But we could respond by asking how profitable and how practical would such an enterprise have been?

First, consider that "information merchants" would have had to purchase the physical records (that were publicly available). These merchants would then have had to hire legions of clerks to convert the purchased data into elec-

tronic form, sort the data according to some scheme, and finally prepare it for sale. This process, in addition to being highly impractical in terms of certain physical requirements, would hardly have been a profitable venture given the amount of labor and cost involved. So, most likely, it would not have occurred to entrepreneurs to engage in such a business venture prior to the advent of sophisticated information technology. But again, we should ask why public records, including records that contained personal information about individuals, were made "public" in the first place.

In order for governmental agencies at the local, state, and federal levels to operate efficiently, records of certain kinds of personal information were needed to be readily available for access. For example, municipal governments needed certain information for tax-assessment purposes, such as assessing tax rates for houses and commercial real estate. State governments needed information about motor vehicles registered in a particular state as well as information about the residents of that state that are licensed to drive those vehicles. And federal governments needed relevant information as well. Those records had to be accessible to governmental agencies at various levels and had to be able to be transferred and exchanged relatively easily. Since the records in question contained personal information that was generally considered to be neither confidential nor intimate, there were good reasons to declare them "public records." It was assumed that no harm could come to individuals because of the availability of those public records, and it was believed that communities would be better served because of the access and flow of those records for purposes that seemed to be legitimate. But certain factors have changed significantly. Information-gathering companies now access those public records, manipulate the records in certain ways, and then sell that information to third parties. Was this the original intent for making such information accessible to the public?

It is perhaps interesting to note that there is now an assumption on the part of some in the commercial sector that *because certain records are public, and because the Internet is a public space, all public records ought to be made available online.* According to this line of reasoning, it is not only desirable (for those entrepreneurs) that many records have, as a matter of fact, been electronically converted and placed online, but rather that there is also some kind of legal mandate to place all public records online. One presumption here might be based on our alleged right to know what the government is up to (based on the notion of freedom of information) or to ensure that public information flows freely. However, there have now been several cases in which operating on such a presumption has caused outrage on the part of many citizens, as well as harm to some, which in the case of Amy Boyer resulted in death. So perhaps we should rethink our criteria for what can count as "public records" and for which kinds of personal information should be made publicly available. We should also perhaps develop specific policies regarding the use of search engines with respect to which kinds of personal information should be made available to them.

If Youens had to track down Amy Boyer without the aid of Internet search facilities, would it have made a difference? Would he have gone to the relevant municipal building to acquire information about Boyer (or would he possibly have hired a private detective to do so)? If Youens himself had gone to the municipal building, would it have been possible that someone, for example a clerk in one of the offices, might have noticed that Youens was behaving strangely? If so, would such an observation have prompted the clerk to notify his or her supervisor or possibly even the police? And would such an action, in turn, possibly have helped to avoid the tragic outcome of the Boyer case? Of course, these kinds of questions are each speculative in nature. And because we are focusing here on the Boyer incident, it is difficult to say what the answers to these questions would mean in a broader sense with regard to cyberstalking and to the easy access of public records. But these questions do give us some pause, and they may force us to reconsider our current beliefs about the public vs. private realm of personal information. These questions also cause us to consider the need for implementing explicit policies with regard to use of Internet search engines in the retrieval of personal information. It is in these senses, then, that the Amy Boyer incident raises for us some more general concerns about personal privacy on the Internet, especially in light of the absence of an explicit policy regarding online search facilities and personal information.

So what can we conclude so far with respect to Amy Boyer's rights and expectations regarding privacy? Was her privacy violated; and if so, in what sense? Amy Boyer's stepfather, Tim Remsberg, believes that his stepdaughter's privacy was indeed violated. He has appeared before congressional groups and has influenced those in congress to sponsor legislation that would make it illegal to sell the social security numbers of one or more individuals as a part of online commercial transactions. Remsberg has

also sued Docusearch.com, the online company that provided Youens with information about where Boyer lived and worked. Additionally, Remsberg has filed a wrongful death suit against Tripod and Geocities, the two ISPs that hosted the Web sites that Youens set up about Boyer. This brings us to our second principal ethical question for consideration in the Boyer case, viz., whether ISPs should be held morally responsible for the harm (psychological as well as physical) that results from the content included on certain Web sites that they happen to host.

4. INTERNET SERVICE PROVIDERS: QUESTIONS OF MORAL RESPONSIBILITY AND LEGAL LIABILITY

As noted earlier, Youens set up two Web sites about Amy Boyer: one containing descriptive information about Boyer, as well as a picture 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? This question is one which is very complicated and which would benefit from being broken down into several shorter questions. To answer the larger question at issue, 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 (of individuals), such as an ISP. We begin with a brief description of some current thinking on the role of responsibility involving ISPs, including a brief analysis of recent laws as well as some recent court challenges to those laws.

Deborah Johnson (2001) provides an excellent overview of background issues involving questions of accountability and responsibility as they pertain to ISPs. So there is no need for us to repeat that discussion here. We will however, comment on certain points, elaborated upon in much more detail in Johnson's exposition, which are especially relevant to our analysis of the Amy Boyer case. In the 1995 case of *Stratton Oakmont v. Prodigy Services Company*, a court found that Prodigy could be held legally liable since it had advertised that it had "editorial control" over 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 much like a newspaper, in which case the standard of strict legal liability used for original publishers could be applied. In light of the case involving Prodigy, 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.

In Section 230 of the Communications Decency Act (CDA), the role of ISPs was interpreted in such a way that would appear to protect ISPs 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 CDA was overturned by a court in Philadelphia, and was eventually struck down by the US Supreme Court, Section 230 of that ACT has remained in tact. (Some have since referred to this policy as the "Good Samaritan immunity for ISPs.") 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 and list servers — they have nonetheless been encouraged to monitor and filter, to the extent that they can, the content of these sites and their electronic forums.

In the preceding paragraph we focused primarily on the legal aspect of responsibility or accountability of ISPs, with particular attention to strict liability laws. We saw that from a legal point of view, ISPs are currently immune from prosecution for the content that can be included on the Web sites and in the other electronic forums that they host. However, we have not yet considered whether ISPs might be held morally accountability, irrespective of the recent court rulings on the legal status of this matter. Deborah Johnson (2001) has noted that while it might be easier to make a utilitarian case for why ISPs could be held legally liable for certain content, it would be much more difficult to make the case that ISPs should be morally responsible for the behavior of their customers. Anton Vedder (2001) has recently advanced an argument for why we should consider holding ISPs morally responsible, as well as legally liable, for harm caused to individuals.

Although we will not do justice to Vedder's argument in the space provided to it in this paper, we will attempt to reconstruct certain aspects of his overall argument in a way that reveals certain controversial points that are salient in the Boyer case. Essentially, Vedder argues that in

order to understand more clearly the issues at stake in this dispute over ISP responsibility, we have to distinguish between two senses of moral responsibility: *prospective* and *retrospective* responsibility. While the latter sense of responsibility is one that is often viewed as "backward looking," the former is sometimes described as "forward looking." Vedder admits, however, that this distinction is not always as clear and unambiguous as its proponents suggest. For example, Vedder points out that it is difficult to hold someone responsible for an *act X* in a retrospective sense if that person were not also responsible for *act X* in some prospective sense as well. Nonetheless, Vedder believes that this distinction is useful in helping us to understand the relevant aspects of moral responsibility necessary to frame an argument in which moral responsibility for harm can plausibly be said to apply to ISPs. But how exactly does Vedder propose that such an argument be constructed?

In the case of ISPs, the threat of legal liability can — despite the fact that currently in the US it is not — be used to deter ISPs from becoming lax about "policing" their electronic forums to some reasonable extent. For example, the threat of some form of legal liability might cause ISPs to monitor or filter their sites on a regular basis to discover controversial sites and to remove them. So underlying the reasoning for the application of liability in a legal sense to ISPs is the utilitarian notion of deterring harm to individuals in the future, a notion of responsibility that is also *prospective* in nature. But Vedder notes that we are hesitant to attribute a retrospective sense of responsibility to ISPs when evaluating their moral culpability because that sense of responsibility also implies *guilt* and because the notion of guilt is usually attributed to individuals and not to organizations. (Guilt, as Vedder also notes, is more often associated with Kantian theories than with utilitarian theories.) Vedder then suggests that in some cases it would also make sense to attribute the notion of guilt to a collectivity (i.e., a collection of individuals) like an ISP, as well as to individuals. This form of attribution of moral responsibility in the retrospective sense to an ISP would also make sense, from Vedder's view, because of the connection Vedder draws (as we discussed above) between retrospective and prospective responsibility. If we reconstruct Vedder's argument, the reasoning would proceed along lines similar to the following: If collectivities (such as ISPs) can be held responsible in a prospective sense (which is the rationale at the basis for legal liability for ISPs), and if it makes no sense to hold an agent responsible for an act in a retrospective sense if he/she is not responsible for that act in a prospective sense as well (as Vedder separately argues), then we could conclude that it is reasonable to ascribe retrospective responsibility in a moral sense to ISPs. Of course, Vedder's argument is far more complex and much more subtle with respect to important details than in the summary account of it that we have reconstructed here.

Let us next consider how we might apply Vedder's argument to the case involving Amy Boyer. Should Tripod and Geocities, the two ISPs that enabled Liam Youens to set up his Web sites about Amy Boyer, be held morally responsible for the harm — to Amy Boyer that resulted in her death? And should those two ISPs be held morally responsible, even if no legal charges (e.g., in terms of strict legal liability) can be brought against them? Of course, we could ask what would be the purpose of attributing moral responsibility to these two ISPs, if there were no "teeth" in the form of legal sanctions that could subsequently be enforced. One answer to this question, though admittedly an answer that might seem to some as one that is trivial or pointless from the vantage-point of law enforcement, is that doing so might cause us not only to distinguish moral from legal considerations in our thinking but could also cause us to think about moral responsibility, both at the individual and collective levels, independent of the presence or absence of particular laws that might or might not apply in a specific case. For example, we can consider whether Tripod and Geocities should be excused from any sense of moral responsibility in the Amy Boyer case simply because these two ISPs cannot be found legally liable and thus prosecuted on legal grounds.

We will also consider in the following section of this essay a variation of the question raised in the preceding paragraph. There, for example, we will consider whether we should automatically excuse ourselves as individuals from being morally responsible in a particular situation simply because there is an absence of a specific law obligating us to perform a certain action in that situation. Even if, as individuals, we would have had no legal obligation to inform Amy Boyer that a death threat involving her had been posted on the Web, does it follow that we also would have no moral responsibility to do so if we had the ability to do so?

So if Vedder is correct, it would seem to follow that aspects of moral and legal responsibility might not be able to be separated as "cleanly" as many philosophers and legal scholars have suggested. While Geocities and Tripod might both be found not to be legally liable for the

harm caused to Amy Boyer, and even though these two ISPs did not deliberately cause her harm, it is not clear that we can conclude that both ISPs should not be held morally responsible in some sense for the harm that resulted to Amy Boyer. It would be plausible to assume, then, that: If Tripod and Geocities could be held legally responsible in a prospective sense of responsibility (based on a utilitarian notion of deterrence), and if prospective responsibility also implies retrospective responsibility (in which case, guilt can be assigned to a moral agent), then we can reasonably infer that the two ISPs in question might deserve at least some of the blame in a moral (even if not in a legal) sense for what happened to Amy Boyer.

5. MORAL OBLIGATION AT THE LEVEL OF INDIVIDUALS

Let us now take up the question of individual moral obligation and ask, what responsibilities Internet users have to inform "would-be victims" of their immanent danger to online stalkers? For example, 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 under a moral obligation to do so? If we want to be responsible, or at least caring citizens, in cyberspace, the answer would seem to be *yes*. It would not be morally permissible to wait for stalking activities to move into physical space before we took any action.

Various proposals for controlling individual behavior in online society have resulted in a conflict between those who wish to regulate 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. "restrictive" one. In the case of cyberstalking, should our duty, if we have one, to assist others be based on legal regulations or should it rest on grounds of individual moral obligation to assist others?

What exactly is meant by "moral obligation?" Historically, philosophers have offered diverse, and sometimes competing, definitions of what is meant by this expression. An Internet user consulting a dictionary to locate a colloquial definition would likely discover one similar to the following: "[moral obligation is] founded on the fundamental principles of right conduct rather than on legalities enactment or custom" (Random House, 1973). Of course, philosophers have attempted to give us far more rigorous definitions of "moral obligation." An interesting question is whether our notion of moral obligation is one that is derived from our concept of justice, or whether instead our sense of "justice" derives from moral obligation. This, obviously, is a complex question and is one that cannot be satisfactorily discussed and answered in this paper. Of course, the question of which moral notion – obligation or justice — is more fundamental could help us to get a clearer sense of exactly what is at stake in disputes involving individual moral responsibility. Contemporary philosophers and ethicists as diverse as Josef Peiper (1966), Carol Gilligan (1982), and Anton Vedder (2001) have explored this question. Unfortunately, in this paper we cannot consider in detail the various points of view that have been put forth by these three thinkers. Nonetheless, we will attempt to sketch out some of the general aspects of their arguments to support a view of individual moral obligation.

Josef Pieper (1966) has argued that the concept of moral obligation is one that is not only "personal" but also linked to one's community. For Peiper, "doing good" is more than obeying some abstract norm (i.e., some Kantian abstract notion of duty and universality). Rather, it is about the individual's relationship to other individuals and to the community itself. Carol Gilligan (1982) first proposed a position similar to Peiper's in a theory of feminist ethics. Both Pieper and Gilligan suggest that justice is a complex concept that goes far beyond the notion of an individual simply obeying laws. Instead, justice involves the *relationship* of individuals, including their individual moral obligations to one another. In the writings of both Peiper and Gilligan, despite their very different objectives, can be found the basis for the thesis that individuals are interconnected and that these individual relationships play a primary role in the development of the concept of moral responsibility. The notion of moral obligation is seen as extending beyond the self to others, both in Pieper's concept of "commutative justice" and Gilligan's "ethic of care". This "ethic of care," as it is labeled in feminist ethics, is more than a mere "non-interference ethic." Rather, it is concerned with "what is above and beyond the floor of duty"(Held, 1995). Based on the belief that care and justice are part of the same moral framework, it has been argued that individuals have a moral obligation to assist others and to prevent harm. From this perspective, individuals would be compelled to act from a basis of moral obligation, even though there may be no specific laws or rules to prescribe such actions.

Anton Vedder (2001) has recently put forth a theory of moral obligation that also has implications at the level of the individual. From Vedder's view, it would seem to follow that we cannot excuse ourselves from our moral responsibility to inform the victim of a threat to his/her life simply because there is no specific law obligating us to do so. Vedder asserts that "the sheer ability and opportunity to act in order to avoid or prevent harm, danger, and offense from taking place" puts an obligation on the agent. We saw in the preceding section how Vedder's argument can be applied to issues of moral responsibility involving organizations. He also points out that in cases "when harm, danger or offense would be considerable while the appropriate action would not present significant risks, costs or burdens to the agent," the same notion of moral responsibility applies, regardless of whether the *agent* is a natural person or an organization (Vedder, 2001).

5.1 A Minimalist Sense of Moral Obligation

Some have argued that while morality can demand of an agent that he or she "do no harm" to others, it cannot *require* the agent to actively "prevent harm" or "do good." In one sense, to do no harm is to act in accordance with moral obligation. 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 always be required to do so? And, if the answer to this question is yes, what are the grounds for such a theory of obligation.

There are a number of theoretical perspectives that would support the view 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. For an interesting account of this type of moral theory, see Louis Pojman (2001). Unfortunately, we are not able to develop Pojman's argument here, since doing so would take us beyond the scope of this paper. But we can at least now see how, based on a model like Pojman's, one might develop a fuller theory in which individuals have an obligation to prevent harm or a "duty to assist." Of course, 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 individual moral obligation.

5.2 Expanding the Sphere of Moral Obligation: *The Duty to Assist*

Questions involving one's "duty to assist" received considerable attention in the notorious Kitty Genovese case in 1964. Genovese was a young woman who was murdered on her street in Queens, New York, as thirty-eight of her neighbors watched. They did not call the police during the 35-minute period of repeated stabbings. This refusal to assist has since become known as "the Genovese Syndrome" (Dorman). Police involved in the Genovese case stated that they believed that even though there was no formal law or specific statute requiring people who saw the crime to call the police, these witnesses were nonetheless morally obligated to do so.

We can draw an analogy between the Genovese case and the Boyer case. The world of cyberspace with its attendant anonymity makes it easy for those who wish to avoid a duty to assist. But, what will cyberspace become, if people do not take their moral obligations seriously? Is our obligation merely to do no harm? Pieper, Gilligan and Vedder would answer *no*. We can see that balancing the harm that could come from doing nothing, which would cause considerable danger to the victim, against the level of inconvenience caused to self, which would be minimal, is yet another motivation for Internet users to assist. In the case of 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 sense of individual moral responsibility was not apparent since certain online users had indeed viewed the Youens' Web site and did not inform Amy Boyer that she was being stalked. As in the case of Kitty Genovese, Boyer was also murdered. Was Boyer's death an online manifestation of the "Genovese syndrome?"

In light of what happened to Amy Boyer, we suggest that online users adopt a notion of individual responsibility to assist others. Doing so would help to keep cyberspace a safer place for everyone, but especially those who are particularly vulnerable: women and children. One might argue that, the threat to Boyer was virtual — i.e., since the threat was not in physical space, it need not have been taken seriously. To accept this argument, we would have to assume that no threats in cyberspace have ever resulted in harm to or in the death

of the victim. Of course, there have been many cases of stalking, including the Boyer and Barber cases, as well as instances of pedophilia, that have resulted in physical harm to individuals. In avoiding our individual duty to assist, individual users disconnect themselves from their responsibility towards fellow human beings. When we accept the duty to assist, we are acknowledging our moral obligation to help prevent others from being harmed.

CONCLUSION

In this study, we have considered some of the salient moral issues involving cyberstalking in general, and the Amy Boyer case in particular. We have seen how, in the Boyer case, cyberstalking has raised certain kinds of concerns for personal privacy that go beyond earlier privacy concerns involving the use of computer technology. Because of the kinds of moral concerns raised in the Boyer case, we considered questions having to do with where exactly the sphere and the scope of moral responsibility should lie in cyberstalking incidents in general. We argued that both Internet Service Providers (ISPs) and individual online users should assume moral responsibility, each in different ways. Although we do not purport to have laid out a definitive answer to the question of how this should be done, and although we recognize the difficulties inherent in defending arguments for moral responsibility at both the organizational and individual levels, we offer a brief argument for why individuals should act to prevent harm from coming to others. That is, we believe that ordinary users have a "duty to assist" others to the extent that they can prevent harm from coming to their fellow users, wherever (or whenever) it is in their power to do so.

Acknowledgments

Significant portions of Sections 2 and 3 of the present paper are extracted from H. T. Tavani *Introduction to Cyberethics: Concepts, Cases, and Controversies* (forthcoming from John Wiley & Sons Publishers). We are grateful to Wiley for permission to use that material in this paper.

This paper expands upon an earlier work, entitled "Is Cyberstalking a Special Type of Computer Crime?" which was presented at the Ethicomp 2001 Conference in Gdansk, Poland, June 2001. We are grateful to participants at that conference, especially to Anton Vedder, for some very helpful comments and suggestions that we received. 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.

References

1999 Report on cyberstalking: a new challenge for law enforcement and industry. www.cybercrime.gov.

California Civil Code 1708.7, http://www.haltabuse.org/laws.html

Dorman, Michael "The Killing of Kitty Genovese". www.lihistory.com.

Foote, D. "You could get raped", *Newsweek*, Vol. 133, No. 6, Feb 8, 1999, p. 64-65.

Gilligan, Carol, *In a Different Voice*, Harvard University Press, 1982.

Grodzinsky, Frances and Herman T. Tavani, "Is Cyberstalking A Special Type of Computer Crime?"*Proceedings of Ethicomp 2001*, Gdansk, Poland, June 2001, Vol. 2, pp.72-81.

Greenberg, P. "Public Internet, Private Lives," *State Legislatures*, Vol.27, No. 2, February, 2001, pp. 39-42.

Hatcher, Colin Gabriel. *CYBER STALKING.* www.safetyed.org.

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

Hitchcock, J.A."Cyberstalking", *Link-Up*, Vol. 17, No. 4, July/August 2000, www.infotoday.com/lu/jul00/hitchcock.htm.

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

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

Nissenbaum, Helen. "Protecting Privacy in an Information Age: The Problem of Privacy in Public," *Law and Philosophy*, Vol. 17, 1998, pp. 559-496.

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

Random House Dictionary of the English Language, Random House, 1973.

Pieper, Josef, *The Four Cardinal Virtues*, University of Notre Dame Press, 1966.

Tavani, Herman T. "Internet Search Engines and Personal Privacy." In *Proceedings of the Conference: Computer Ethics - Philosophical Enquiry (CEPE '97)*. Rotterdam, The Netherlands: Erasmus University Press, 1998, pp. 214-223.

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

Tavani, Herman T. "The Uniqueness Debate in Computer Ethics: What Exactly is at Issue, and Why Does it Matter?" Paper presented at the CAP 2001 Conference, Carnegie Mellon University, Pittsburgh, PA (USA), August 10, 2001. Forthcoming in *Ethics and Information Technology*.

"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, "Accountability of Internet Access and Service Providers – Strict Liability Entering Ethics," *Ethics and Information Technology*, Vol. 3, No. 1, 2001, pp. 67-74.