6-2002

Cyberstalking, Personal Privacy, and Moral Responsibility

Herman T. Tavani
Rivier College

Frances Grodzinsky
Sacred Heart University

Recommended Citation

Grodzinsky, F. S., & Tavani, H. T. (2002). Cyberstalking, personal privacy, and moral responsibility. *Ethics and Information Technology, 4*(2), 123-132.

Ethics and Information Technology **4:** 123–132, 2002.

Cyberstalking, personal privacy, and moral responsibility

Herman T. Tavani[1]* and Frances S. Grodzinsky[2]
[1]*Department of Philosophy, Rivier College, 420 Main Street, Nashua, NH 03060, USA;* [2]*Department of Computer Science and Information Technology, Sacred Heart University, 5151 Park Ave., Fairfield, CT 06432, USA (*author for correspondence, E-mail: htavani @rivier.edu)*

Abstract. This essay[1] examines some ethical aspects of stalking incidents in cyberspace. Particular attention is focused on the Amy Boyer/Liam Youens case of cyberstalking, which has raised a number of controversial ethical questions. We limit our analysis to three issues involving this particular case. First, we suggest that the privacy of stalking victims is threatened because of the unrestricted access to on-line personal information, including on-line public records, currently available to stalkers. Second, we consider issues involving moral responsibility and legal liability for Internet service providers (ISPs) when stalking crimes occur in their 'space' on the Internet. Finally, we examine issues of moral responsibility for ordinary Internet users to determine whether they are obligated to inform persons whom they discover to be the targets of cyberstalkers.

Key words: cyberstalking, duty to assist, Internet search engines, Internet service providers, legal liability, moral responsibility, personal privacy, public records

Cyberstalking: An introduction and overview

What exactly is cyberstalking, and how 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*, 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 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 on-line world. On the one hand, we do not claim that cyberstalking is a new kind of crime.[2] On the other hand, we believe 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 on-line. In addition, a cyberstalker can stalk one or more individuals from the comfort of his or her home, and thus 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.

Many people have become concerned about the kind of stalking-related activities that have recently occurred in cyberspace, and there are several reasons why these individuals would seem justified in their concern. Because stalking crimes in general are not fully understood in terms of their conceptual boundaries and their implications, it is that much more difficult to comprehend exactly what it would mean to commit a stalking crime in the cyber-realm.

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' 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

[1] An earlier version of this paper was presented at the CEPE 2001 Conference, Lancaster University, UK, December 14–16, 2001. The present paper expands on two earlier works (Grodzinsky and Tavani, 2001, 2002). Portions of this article are extracted from H.T. Tavani, *Ethics in an Age of Information and Communication Technology* (forthcoming from John Wiley & Sons Publishers). We are grateful to Wiley for permission to use that material in this paper.

[2] Nor do we argue that cyberstalking is a 'genuine computer crime.' See Tavani (2000) for some distinctions that can be drawn between genuine computer crimes and computer-related crimes.

that was displayed through 'the cross hairs of a rifle.' Using various pseudonyms, Hunold corresponded with several 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. 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?'

The case of Randi Barber and Gary Dellapenta also illustrates a criminal incident that has sometimes been included under the category of cyberstalking. In this particular case, the stalker himself engaged others to stalk his 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 telephone solicitations from men, and in one instance, a 'solicitor' actually appeared at the door of her residence. Barber had no idea how potentially dangerous her situation was. For example, she was not aware 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.' Having access to chat rooms and message boards, Dellapenta was able 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. Once again, however, we can ask whether the Barber/Dellapenta incident is a genuine case of cyberstalking or whether it is an instance of a more general case of harassment in cyberspace.

Thus far we have briefly described two different kinds of criminal incidents that some have referred to as examples of cyberstalking. 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 is a clear instance of cyberstalking. We will also see why the Boyer case introduces a range of questions worthy of ethical consideration.

Some ethical reflections on the Amy Boyer 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 many of the stalking activities that eventually led to Boyer's death by using a variety of online tools available to him. Through the use of standard Internet search facilities, and related online tools, Youens was able to find out where Boyer lived, where she worked, what kind of vehicle she drove, and so forth. In addition to using Internet search-related tools to acquire personal information about Boyer, Youens was also able to take advantage of other kinds of online facilities, such as those 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 has raised some controversial questions, many of which would seem to have significant moral implications for cyberspace. But is there anything special about the Amy Boyer case from an ethical perspective? 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 simply as 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 certain aspects of cyberstalking raise special problems that challenge our conventional moral and legal frameworks. For example, one could point out that 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. We leave open the question whether any of the ethical issues involving cyberstalking are new or unique.[3] Instead, we focus on some ways in which cyberstalking challenges our existing moral framework.

We have argued elsewhere (see Grodzinsky and Tavani, 2002) that cyberstalking activities have significant implications for a range of ethical and social issues, including security, free speech, and censorship. In this essay, we argue that cyberstalking also raises questions involving personal privacy, moral responsib-

[3] For an in-depth discussion of the question whether cyberstalking has introduced any unique ethical issues, see Tavani (2002).

ility and legal liability. Our primary focus, however, is on some of the ways that these particular ethical issues impact the Amy Boyer case. 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 permitted 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 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?

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 the remainder of this essay to three ethical concerns involving the Amy Boyer case. First, we examine certain kinds of privacy threats posed to cyberstalking victims because of the unrestricted access to personal information included in on-line public records. We then consider questions of legal liability and moral responsibility for Internet service providers (ISPs) with respect to cyberstalking incidents that occur in their 'space.' 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.

Internet search engines, public records, and personal privacy

Consider the useful, and arguably important, function that Internet search engines provide in directing us to online resources involving academic research, commerce, recreation, and so forth. Hence, some might be surprised by the suggestion 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 on whom an on-line search is conducted. But one might still ask why exactly the use of search-engine technology is controversial with respect to the privacy of individuals. Consider that an individual may be unaware that his or her name is among those included in one or more databases accessible to search engines. Because of this, individuals have little, if any, control over how information about them can be made available and be disseminated across the Internet.[4] 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. It should be noted that Boyer neither placed any personal information about herself on the Internet, nor was she aware that such information about her had been so listed.

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. Traditionally, information about persons that is available to the general public has not been protected by privacy laws and policies. We can, of course, question whether all of the information currently available on the Internet should be treated as 'public information' that deserves no normative protection?

Because of concerns related to the easy flow of personal information between and across databases, certain laws have been enacted 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.'[5] 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,

[4] For a more detailed discussion of privacy problems that can arise from certain uses of Internet search engines, see Tavani (1998).

[5] See also Nissenbaum (1997) for a discussion of some of the challenges that information technology poses for the 'problem of privacy in public.'

by default, as information that does not warrant normative protection. Is this presumption about non-intimate personal information that is publicly available on the Internet one that it is either reasonable or fair? Was it fair to Amy Boyer?

The commodification of personal information in public records

With respect to privacy policies and laws in the Internet age, what status should be accorded to personal information that resides in public sources, such as in public records? Consider that in the era preceding the Internet, information of this particular kind could be acquired by individuals who were willing to travel to municipal buildings and, where applicable, pay a small fee for a copy of the desired records. If this kind of information was already available to the general public before the advent of cyber-technology, why should its status necessarily change because of the new technology? Perhaps an equally important question is: Why were such records made public in the first place? For example, were they made public so that on-line 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 such an enterprise would have been.

First, consider that 'information merchants' would have had to purchase copies of the physical records (that were publicly available). These merchants would then have had to hire legions of clerks to convert the purchased data into electronic 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 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 who 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.[6] Was this the original intent for making such information accessible to the public?

A questionable inference

Many information merchants seem to believe that because: (a) *public records have always been available in a public space*; and (b) *the Internet is a public space*; it follows that (c) *all public records ought to be made available online.* According to this line of reasoning, it is not only a good thing that many public records have, in fact, been placed online; rather it is assumed that municipal governments should be required to make *all* public records available online. Defenders of this view often proceed on the reasoning that, as citizens, we have a right to know what the government is up to (based on the notion of freedom of information). Placing public records online, they further assume, will ensure that such 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,[7] as well as harm to some, which in the case of Amy Boyer resulted in death. So perhaps we should rethink our policies regarding access to on-line public records. We should also perhaps develop specific policies and guidelines

[6] Richard De George (2001) has suggested that because Internet and computing technology has made it possible for organisations and individuals to gather information in ways that were not possible in the pre-Internet era, we need to reconsider why societies have public records and how those records should be protected.

[7] For example, Michael Scanlan (2001) describes a controversial case involving the state of Oregon, which sold records in its Motor Vehicle Registry database to an on-line consulting business. The citizens of Oregon complained and the state eventually reversed its policy regarding the sale of information about its licensed drivers.

regarding which kinds of personal information should be made available to search engines.

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, each of these questions is speculative in nature.[8] 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.

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 the US 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 the second of our three main ethical question for consideration in the Boyer case: Should ISPs 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?

[8] Richard De George (2001) points out that when public records were accessible only in public buildings, there was a much easier way of tracing the acquisition of those records in the event that some 'misuse' had been made of the information contained in them.

Internet service providers, legal liability and moral responsibility

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? Because this question is one which is very complex, it 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 organisation 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.

ISPs and legal liability

Deborah Johnson (2001) provides an excellent overview of the 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 briefly on certain points that are a elaborated in much more detail in Johnson's text but that 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 similar to 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 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 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.

ISPs and moral responsibility

In the preceding section we focused primarily on the legal aspect of the responsibility or accountability of ISPs, with particular attention to strict liability laws. We saw that from a legal point of view, ISPs in the US 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 accountable, 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 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 *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 be used – despite the fact that currently in the US it is not – 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 then possibly 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, an aspect 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 between retrospective and prospective responsibility (as we discussed above). Reconstructing Vedder's argument slightly, 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.[9]

Applying Vedder's argument

Consider how Vedder's argument can be applied to the case involving Amy Boyer. Should Tripod and Geocities, the two ISPs that enabled Liam Youens to

[9] We should point out that Vedder's argument is more complex than the version we have reconstructed for purposes of this paper. We should also point out that as in the case of Nissenbaum (1995), Vedder believes that the motion of moral responsibility can be understood in a broader sense; and as in the case of Spinello (2001), Vedder believes that I & Ps should be held morally accountable. However, Vedder's argument differ in important respects from both Nissenbaum's and Spinello's.

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 the purpose would be in 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 to distinguish between certain moral and legal considerations in our thinking. And it might 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 final section of this essay a variation of the question raised in the preceding paragraph. There 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 it were in our power to inform her?

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.

Moral obligation at the level of individuals

We now consider the question of individual moral obligation, by asking what kinds of 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, is that user 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*. In this case, 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 Dictionary*). 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, we are not able to examine the three positions in the depth that each deserves. Nonetheless, we sketch out some general themes in their respective arguments.

Three views of moral obligation: The Peiper, Gilligan, and Vedder models

Josef Peiper (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), in her work in feminist ethics, first proposed a position similar to Peiper's. Both Peiper and Gilligan suggest that moral obligation goes far beyond the notion of an individual simply obeying laws. For them, moral obligation is closely tied with a more complex concept of justice. As such, 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.' 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.[10]

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 organisations. 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 organisation (Vedder, 2001).

A minimalist notion 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.

A number of theoretical perspectives 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 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 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.

*Expanding the sphere of moral obligation: The **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. A young woman, Genovese 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

[10] For a discussion of some ways in which Gilligan's system of ethics can be applied to issues involving cyberstalking, as well as to issues in computer ethics in general, see Alison Adam (2001, 2002).

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., morally obligated to assist). We can also ask what kind of place cyberspace will become, if people refuse to assist users who may be at risk to predators and murderers. Is our obligation to our fellow users one in which we are required merely to do no harm? Peiper, Gilligan and Vedder would each answer *no*. Consider the potential harm that could come from doing nothing vs. the level of inconvenience caused to self, which would be minimal, by coming to the assistance of others who may be in danger in cyberspace. 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 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 for women and children who are particularly vulnerable groups. Some might be inclined to argue that the threat to Boyer was merely virtual, since the threat itself did not occur in physical space.[11] Such an argument, however, ignores the fact that threats in virtual space have, in fact, resulted in physical harm to individuals. In addition to the harm resulting in cyberstalking cases, consider the physical harm that has resulted to some victims of Internet pedophilia. In avoiding our individual duty to assist, individual users disconnect themselves from their responsibility towards fellow human beings. When they accept the duty to assist, they are acknowledging their moral obligation to help prevent others from being harmed.

Conclusion

We have examined some ethical aspects of cyberstalking in general, and the Amy Boyer case in particular. We saw that the cyberstalking case involving Boyer raised privacy concerns that cause us to reconsider the kinds of protections currently accorded to on-line public records. We also saw that cyberstalking issues have raised questions for ISPs having to do with legal liability and moral responsibility. It was argued that issues of moral responsibility involving cyberstalking span two spheres: the collective (e.g., ISPs) and the individual (i.e., ordinary Internet users). We believe that both ISPs and individual users, each in different ways, should assume some moral responsibility for preventing harm from coming to individuals targeted by cyberstalkers. Although we recognise the difficulties inherent in defending arguments involving moral responsibility at both the collective and individual levels, we nonetheless offer some preliminary suggestions for why both organisations (such as ISPs) and individuals should act to prevent harm from coming to their fellow Internet users, whenever it is in their power to do so.

[11] This type of reasoning is a variation of what James Moor (2001) refers to as the 'virtuality fallacy.' According to this particular line of fallacious reasoning: *X* exists in cyberspace; cyberspace is not in the real world; therefore, *X* is exempt from the demands of the real world.

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.

Bibliography

Alison Adam. Cyberstalking: Gender and Computer Ethics. In Eileen Green and Alison Adam, Editors, *Virtual Gender: Technology, Consumption, and Identity*, pages 209–234. Routledge, London, 2001.

Alison Adam. Cyberstalking and Internet Pornography: Gender and Gaze. *Ethics and Information Technology*, 4(2): 133–142, 2002.

Richard T. De George. Law and Ethics in the Information Age. A paper presented at Rivier College, Nashua, NH, April 3, 2001.

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

Frances S. Grodzinsky and Herman T. Tavani. Is Cyberstalking a Special Type of Computer Crime? In Terrell Ward Bynum, et al., editors, *Proceedings of ETHICPMP 2001: The Fifth International Conference on the Social and Ethical Impacts of Information and Communication Technology*, Vol. 2, pages 72–81. Wydawnicktwo Mikom Publishers, Gdańsk, Poland, 2001.

Frances S. Grodzinsky and Herman T. Tavani. Cyberstalking, Moral Responsibility, and Legal Liability Issues for Internet Service Providers. In Joseph Herkert, editor, *Proceedings of*

ISTAS 2002: The International Symposium on Technology and Society, pages 331–339. IEEE Computer Society Press, Los Alamitos, CA, 2002.

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

James H. Moor. Reason, Relativity, and Responsibility in Computer Ethics. *Computers and Society*, 28(1): 14–21, 1998.

James H. Moor. Just Consequentialism. A paper presented at the 2000–2001 Rivier College Humanities Lecture Series, Nashua, NH, February 20, 2001.

Helen Nissenbaum. Computing and Accountability. In Deborah Y. Johnson and Helen Nissenbaum, Editors, *Computing, Ethics and Social Values*, pages 526–538. Englewood Cliffs, NJ, Prentice Hall, 1995.

Helen Nissenbaum. Toward an Approach to Privacy in Public: Challenges of Information Technology. *Ethics & Behavior*, 7(3): 207–219, 1997.

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

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

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

Michael Scanlan. Informational Privacy and Moral Values. *Ethics and Information Technology*, 3(1): 3–12, 2001.

Richard A. Spinello. Internet Service Providers and Defamation: New Standards of Liability. In Richard A. Spinello and Herman T. Tavanii, Editors, *Readings in CyberEthics*, pages 198–209. Sudbury, MA, Jones and Bartlett, 2001.

Herman T. Tavani. Internet Search Engines and Personal Privacy. In Jeroen van den Hoven, Editor, *Proceedings of CEPE '97: Conference on Computer Ethics – Philosophical Enquiry*, pages 214–223. Erasmus University Press, Rotterdam, The Netherlands, 1998.

Herman T. Tavani. Defining the Boundaries of Computer Crime: Piracy, Break-ins and Sabotage in Cyberspace. *Computers and Society*, 30(4): 3–9, 2000.

Herman T. Tavani. The Uniqueness Debate in Computer Ethics: What Exactly Is at Issue, and Why Does It Matter? *Ethics and Information Technology*, 4(1): 37–54, 2002.

Anton H. Vedder. Accountability of Internet Access and Service Providers: Strict Liability entering Ethics. *Ethics and Information Technology*, 3(1): 67–74, 2001.