Is There a Place for Cyberethics? A Conceptual Look at the Effects of Cybertechnology on Ethics and Communications in Cyberspace

Seyed Mahmood Farjami
School of Communication, Universiti Sains Malaysi (USM)
11800 Pulau Pinang, Malaysia
E-mail: M_farjami@yahoo.com

Received: November 2, 2011 Accepted: November 29, 2011 Published: April 1, 2012
doi:10.5539/ass.v8n4p148 URL: http://dx.doi.org/10.5539/ass.v8n4p148

Abstract

Cyberethics contains includes morality and law in cyberspace. There are two main ideas concerning cyberethics: one suggests that cyberethics can simply be modeled on the same codes of practice as professional ethics for other technologies. The other asserts that unlike most previous technologies, cybertechnology can be shaped and modeled to perform a variety of functions and therefore requires a new paradigm for applied ethics.

This paper supports the latter assertion and by examining a series of ethical issues in cyberspace tries to show that these ethical problems can be so complicated that they are impossible to consider and understand from outside of cyberspace.

Keywords: Cyberethics, Telecommunications, Cybertechnology, Computer science, Vacuum policy, Cyber journalism

1. Introduction

By definition, briefly, Ethics is the study of morality and morality, or a moral system, can be defined as a system of rules for guiding human conduct and principles for evaluating those rules (Tavani, 2007). Although, there are many theories, cognitive debates and conceptual arguments about ethics, in real life people are reluctant to use the pure aspects of philosophical ethics theories. There are unlimited ethical problems that people face in their lives that must be categorized for study and resolution. Applied ethics examines practical ethical issues. The sorts of questions addressed by applied ethics are common problems in our lives such as: "Is getting an abortion immoral?", "Is euthanasia immoral?", "Is affirmative action right or wrong?", "Do animals have rights as well?" and "Do individuals have the right of self-determination?"

In our society, professional careers often carry with them additional moral responsibilities that go hand in hand with the additional knowledge and experience the profession imparts. For example, a lay person would not be held responsible for neglecting to provide medical care to save a car crash victim because they do not have the relevant knowledge. By contrast, a fully trained doctor (with the correct equipment) would be capable of making the correct diagnosis and carrying out the needed procedure and we would think it wrong if he/she stood by and failed to help in this situation. One cannot be held accountable for failing to do something that he or she does not have the ability to do. In other words, careers that are considered to require a high level of skill and specialized knowledge also tend to carry a high level of special responsibility.

Most professions have internally enforced codes of practice that members of the profession must follow, to prevent exploitation of the client and preserve the integrity of the profession (Tavani, 2007).

For example, medical doctors and military personnel have strict professional codes of ethics, but these codes of ethics are meaningful only in cases that are related to their abilities and professions. Professional ethics has roots in applied ethics, but there is a border between the two. If a physician does something wrong with or to a patient, his/her offense can be judged under professional laws and codes of ethics but if he/she does something wrong to his/her spouse, the offense is judged using the applied ethics standards that all members of a society are held to, not a code specific to a particular profession.

1.1 Cyberspace and Cyberethics

In public use, it seems Cyber doesn't have a clear definition and it is a combination form meaning "computer," "computer network," or "virtual reality," used in the formation of compound words such as cybertechnology, cyberspace, cyberethics, cyberjournalism, and etc..

Also cyber has been defined as 'a prefix used in a growing number of terms to describe new things that are being made possible by the spread of computers, and cyberspace is a metaphor for describing the non-physical terrain created by computer systems' (Webopedia, 2011). Accordingly,"cyberethics" contains morality and law in cyberspace (Spinello, 2006).

By the last decades of 20th century, widespread use of computers generated a series of ethical issues that (a) did not exist before the advent of computing and (b) could not have existed if computer technology had not been invented (Maner, 2004). Although attention to ethical issues related to computers can be traced from its informal beginnings in the 1940s and 1950s (Bynum &Rogerson, 1996), serious formal efforts to determine codes of ethics for computer users and professionals were begun during 80s and 90s. In 1992, Computer Ethics Institute created "The Ten Commandments of Computer Ethics"(1). It copies the style of The Ten Commandments from The Bible and uses the archaic "thou shalt" and "thou shalt not" found in The King James Version (Barquin, 1992).

A few years before that time, Levy (1984) published a book about hacker ethics and had suggested some codes of ethics for hackers. But very soon and especially by the development of the Internet, cyberspace had become so complicated that these kinds of simple regulations were not enough.

During just three decades there were innumerable unethical and illegal acts performed in cyberspace like hacking, cyberfraud, cybersex, unleashing of worms and viruses, Identity theft, cyberterrorism, cyberespionage, cyberpiracy, cybervandalism, denial of service attacks, etc.. Some of these acts have aspects similar to real sphere crimes. For example, cybersex is pornography and/or prostitution via cybertechnology with some variations (not essentially) from real (physical) space that can be provided in cyberspace, like violating the prohibition of access to pornographic contents for people who are under 18. Also, cyberterrorism, cyberfraud, cyberpiracy, cybervandalim and cyberespionage can be defined as committing to do or to design to do terrorism, fraud, piracy, vandalism and espionage acts by using cybertechnology.

But some sorts of unethical issues in cyberspace are too complicated even to be called old issues with new technologies. Moor (2000) points out that computer technology, unlike most previous technologies, is 'logically malleable'; it can be shaped and modeled to perform a variety of functions. He believes because of its logical malleability, cybertechnology can generate 'new possibilities for human action' that appear to be limitless. Some of these possibilities for action generate what Moor calls 'policy vacuums' because people have no explicit policies or laws to guide new choices made possible by computer technology.

1.1.1 The Simple, but not so: Napster Case

The 'Napster' case is one of the most famous cases that presented some issues in cyberspace that were so complicated that they could not be judged either by ordinary ethical and legal standards or by professional, ethical codes of practice. Napster (Napster.com) was an online, music, peer-to-peer file sharing service to which a user could send a request for a song or an album and if someone is online and wanted to share, they could exchange mp3 files. Immediately, Napster was sued for violating the Intellectual property law (Bergen, 2002; Langenderfer & Cook, 2001; Stern, 2000).

Napster responded that its activities were perfectly legal under the fair-use doctrine(2). But finally the court ruled against Napster and the original site ceased operations and later reopened as a pay-per-song web site (Tavani, 2007). However, the Napster case prompted several debates about intellectual property and copyright in cyberspace and numerous articles, books and studies have been written about it showing that this case has remained controversial. (See Bergen, 2002; Carlsson&Gustavsson, 2001; Dogan, 2000; Langenderfer& Cook, 2001; Spitz & Hunter, 2005; Stern, 2000)

1.1.2 Mining the Data - The Usual Suspects

Data mining is another new and serious phenomenon in cyberspace that can cause numerous ethical issues. Data mining involves the indirect gathering of personal information through an analysis of implicit patterns discoverable in data (Rao & Quester, 2006). For instance, some state security agencies in the U.S. use data-mining techniques on American library members (Han, Kamber, & Pei, 2011). Complicated algorithms check all members' information and can recognize who is probably interested in making bombs or terrorist

attacks. One of the best areas for data-mining is the Internet and such techniques are now also used by commercial web sites to analyze data about users, which can then be sold to third parties.

Tavani (2007) believes data-mining activities can generate new and sometimes non-obvious classification or categories; as a result, individuals whose information is mined can become identified with or linked to certain newly created groups that they might never have imagined to exist. In agreement with Moor's idea about 'policy vacuums', Tavani believes data-mining technology raises special concerns for personal privacy, which is not supported by the law on how information acquired through data mining activities is subsequently used.

This kind of reasoning supports cyberethics as a distinct ethics system in cyberspace involving professional and applied ethics. Some, like Gotterbarn, (1995) suggest that the principles focused on in computer ethics should be issues of professional responsibility and not the broader moral and social implications of that technology. He asks why we need to have cyberethics whereas we don't need to have "printing press ethics" or "airplane ethics".

To challenge Gotterbarn's claim that equates cybertechnology with any other technology that at most needs some codes of conduct or the like, cases concerning the essential effects of cybertechnology on cyberjournalism will be discussed. It will be argued that cyberethics must be an ethical system based on its specific technology, and how overlooking the role of this technology in human communications can cause serious problems.

2. Cyberethics and Cyberjournalism, Some Ethical Cases

Cyberspace cannot only be studied as a broadcast medium (Tavani, 2007) but also can involve huge numbers and many kinds of media called cybermedia that are directly connected with cyberjournalism. Cyberjournalism is a term coined after the merging of various traditional media brought about by the proliferation of media industries due to the current influx of cybertechnology and globalization. Cyberjournalism made possible by the cybertechnology has gained importance and is functioning as a pervasive medium along with the traditional media such as print and electronic (Ibrahim, 2002). In the following, several examples of ethical phenomena from real cases will be discussed to demonstrate the unique and complex nature of ethical and legal issues relating to journalism in combination with cybertechnology.

2.1 Abusing from Keywords

Traditionally, a media is responsible, ethically and legally, for the materials it publishes. But in Cyber journalism one is facing a unique phenomenon by which the audience. is seemingly the victim of clever, hidden tactics. The influence of some key words and search engines to increase the number of visitors to a site in the web space has become a serious research problem in cyber media. When words that are of greater interest to the public are more frequently repeated on a page of cyber media, the page has a higher chance of being visited, compared to a page that has used the same words only as many times as needed. As a result, an online journal with more of such pages is being viewed more frequently than other journals.

In this example, and at a deeper level, a kind of online media programming is observed which enables managers of internet media to incorporate in the pages of their journals certain irrelevant but high interest words such as sex, Hollywood, scandal, terror, etc.. These words constitute the content of an irrelevant page which is not visible to the audience during an online search.

Now, the question is whether playing such tricks is ethical. The answer to this question is not that easy because, traditionally a media is only responsible for what it publishes, but in this case nothing has really been published. On other hand, however, this can be legally prosecuted as a case of "cheating in a free competition".

2.2 Link-dumps and Responsibility

Community link dumps are sites with a great number of members from all over the world send materials or links which they find interesting and the members vote on them. In the most popular community link dumps like dig.com and balatarin.com, if a link obtains enough points, it is shown on the first page of the site for every- one (members and visitors) to view upon opening the site. These sites are usually popular because of their variety and some of them have hundreds of thousands of visitors daily. Of course, there have always been media in various fields whose main job it is to collect interesting materials from other media, but they have always had certain legal responsibilities.

In the cyber world, such journals assume no responsibilities, because they claim they do not publish anything independently; they publish links, which are followed if readers are interested in the material. This seems straightforward enough, but what if a site that is not very popular, or a personal weblog, publishes a scandalous piece of news, which is not true. The news is read hundreds of thousands of times due to the link and creates vast effects. The source site is forced to retract the news, but this is not reflected in the link dump or does not gain enough points to go there, making the retraction useless.

2.3 FEEDs and Intellectual Properties

In conventional media, publishing the news, reports and materials of other journals follow(s) certain rules governed by the laws of copyright. Similarly, media such as television and radio can use the products of other media under certain conditions. In all such cases, the main media takes the lead, because either it earns a revenue or adds to its prestige (as the main source) or has acted faster than the others.

This traditional mechanism has changed greatly in cyber media. Now almost all popular cyber media provide the public with their RSS (A general version of FEED). That is, the material they publish is accessible at the same time in other sites. Meanwhile, a certain kind of media has emerged whose activity is to collect and classify the FEEDs from other media.

These media themselves provide other media and people with their general FEEDs or classified FEEDs. This is often done by the media receiving FEEDs as well, and, of course, in every operation, there is the possibility of adding other elements to the main news stories. For example, in the site that links to the main site, comments of the main site may be added to the news and the second site that links to the first site may add pictures and related stuff. Thus a great and complicated network emerges in which the many sites that link to each other find great significance due to technologic facilities (which make it possible to manipulate news stories according to one's taste). As a result, the person receiving the news story may receive a product each part of which comes from a different source. This gives rise to many legal and ethical issues surrounding the authority of a journalistic product.

2.4 Denial of Service Attacks and a Recent Case

An example of an even more complicated case in which ethical and legal judgment based solely on professional ethics for cyberspace was not enough, surrounds the 2009 presidential elections in Iran. During clashes after the election, there was a war of cybermedia between pro-government forces and protesters. In an unprecedented move, the supporters of one of the candidates (Mousavi), decided to paralyze a pro-government news website (Farsnews.com) that they believed spread lies in support of the government. To do so, since the site was auto-refresh, they sat at the computer each day,-opened the main page of said news agency's web site and kept it open for hours, causing a kind of attack to the server of a site named "denial of service attack". Because of the great pressure on the news agency's server processor, it was paralyzed; therefore other people could not see the first page. (See Shachtman, 2009)

The programmers of the news agency's site took a similar measure. They placed a brief software instruction in the site to send a request to the web site of the rival candidate with every visit. As a result, when the rival's site received a great number of requests, its processor faced a similar condition and failed to operate.

3. Conclusion

The examples cited here along with numerous other incidents of questionable ethical cyber action show that cyberethics must be more than just some codes of conduct or even professional ethics. The premise being that ethical problems which depend essentially on cyberspace can be better solved, or at least understood, in cyber sphere with a focus on the essence of cybertechnology. Some like Barlow (1996) who wrote 'A Declaration of the Independence of Cyberspace' in response to the passing into law of the Telecommunications Act of 1996 in the United States, think cyberspace is so different from the physical world that all aspects in this sphere must be considered independently.

In fact cyberspace is growing so fast and involves such a variety of human communications that it is not only facing a 'policy vacuum' but is also probably facing 'conceptual vacuums' or what Moor (2000) calls 'conceptual muddles'.

Cyberspace is a new world built on technology and all its aspects. All communications and creations in this new world are unique because of an inseparable from the medium of technology. The essential nature of this relationship is at the core of the development of cyberethics. Most ethical issues in cyberspace can be appropriately understood and analyzed only by understanding this relationship. Cyberethics cannot be studied, according to ethical systems in the non-cyber world, nor merely as some set of ethical codes of practice with respect to the technology. Further studies, especially interdisciplinary studies between computer science, philosophy and communications, can go forward to understand the technological essence of cyberspace and can positively influence the consideration and solution of ethical issues and other human matters in cyber sphere.

Acknowledgment

I am grateful to Prof. Adnan Hussin for his ongoing guidance and Homa Edalati Fard for her comments on an earlier draft of this article.

References

Barlow, J. P. (1996). A Declaration of the Independence of Cyberspace. Retrieved Oct. 24, 2011, from https://projects.eff.org/~barlow/Declaration-Final.html

Barquin, R. C. (1992). *In pursuit of a 'ten commandments' for computer ethics.* Computer Ethics Institute.

Bergen, G. J. (2002). Napster Case: The Whole World is Listening. *The Transnat'l Law,* 15, 259.

Bynum, T. W., & Rogerson, S. (1996). Global Information Ethics: Introduction and Overview. *Science and Engineering Ethics*, 2(2), 131-136. http://dx.doi.org/10.1007/BF02583548

Carlsson, B., & Gustavsson, R. (2001). The rise and fall of napster-an evolutionary approach. *Active Media Technology,* 347-354.

Dogan, S. L. (2000). Is Napster a VCR--The Implications of Sony for Napster and Other Internet Technologies. *Hastings LJ,* 52, 939.

Gotterbarn, D. (1995). Computer ethics: Resposibility Regained. In D. G. Johnson & H. Niddenbaum (Eds.), *Computing, Ethics, and Social Values.* Upper Saddle River, NJ: Prentice Hall.

Han, J., Kamber, M., & Pei, J. (2011). *Data mining: concepts and techniques.* Waltham: Morgan Kaufmann Pub.

Ibrahim, F. (2002). Cyber journalism: Bridging the gap between professionalism and epistemology. Retrieved Oct. 24, 2011, from http://www.portalcomunicacion.com/bcn2002/n_eng/programme/prog_ind/asp4.asp?id_pre=1162

Langenderfer, J., & Cook, D. L. (2001). Copyright Policies and Issues Raised by A&M Records v. Napster:" The Shot Heard'Round the World" or" Not with a Bang but a Whimper?". *Journal of Public Policy & Marketing,* 280-288. http://dx.doi.org/10.1509/jppm.20.2.280.17367

Levy, S. (1984). *Hackers: Heroes of the Computer Revolution*. Anchor Press.

Maner, W. (2004). Unique ethical problems in information technology. *Computer ethics and professional responsibility*, 39-59.

Moor, J. H. (2000). What Is Computer Ethics? In R. Baird, R. Ramsower & S. Rosenbaum (Eds.), *Cyberethics: Social and Moral Issues in the Computer Age* (pp. 23-33). Amherst, NY: Prometheus Books.

Rao, S., & Quester, P. (2006). Ethical marketing in the internet era: a research agenda. *International Journal of Internet Marketing and Advertising,* 3(1), 19-34.

Shachtman, N. (2009). Web Attacks Expand in Iran's Cyber Battle. Retrieved Oct. 24, 2011, from http://www.wired.com/dangerroom/2009/06/web-attacks-expand-in-irans-cyber-battle/

Spinello, R. A. (2006). *Cyberethics: Morality and law in cyberspace.* London: Jones & Bartlett.

Spitz, D., & Hunter, S. D. (2005). Contested codes: The social construction of Napster. *The information society*, 21(3), 169-180. http://dx.doi.org/10.1080/01972240490951890

Stern, R. (2000). Napster: a walking copyright infringement? *Micro, IEEE,* 20(6), 4-5, 95.

Tavani, H. T. (2007). *Ethics and technology: Ethical issues in an age of information and communication technology* (2nd ed.). Wiley.

Webopedia. (2011). Retrieved Oct. 25, 2011, from http://www.webopedia.com/TERM/C/cyber.html

Notes

Note 1. To see it on the original webpage go http://computerethicsinstitute.org/publications/tencommandments.html

Note 2. The doctrine of *fair use* has developed through a substantial number of court decisions over the years and has been codified in section 107 of the copyright law.

Section 107 contains a list of the various purposes for which the reproduction of a particular work may be considered fair, such as criticism, comment, news reporting, teaching, scholarship, and research. Section 107 also sets out four factors to be considered in determining whether or not a particular use is fair:

1. The purpose and character of the use, including whether such use is of commercial nature or is for nonprofit educational purposes
2. The nature of the copyrighted work
3. The amount and substantiality of the portion used in relation to the copyrighted work as a whole
4. The effect of the use upon the potential market for, or value of, the copyrighted work

(Source: http://www.copyright.gov/fls/fl102.html)