Computer Ethics and its related issues

Dr. Mamta Sareen

Associate Professor, Kirori Mal College, University of Delhi.

Abstract

The evolution of modern society with the unprecedented growth of ICT has resulted in a shift from industrial society towards informational society. This transformation is a multidimensional shift that has impacted almost all aspects of society. The emergence of the virtual world has brought its own rules and culture that has raised questions relating to the age old traditions. This paper concentrates on the emergence and the need of computer ethics in the present world followed by a thorough analysis of three major issues pertaining to cyber ethics namely privacy, social media and Internet related research.

Keyword: computer ethics, privacy, information, social media, Internet research ethics

1. Introduction

With the phenomenal growth of the World Wide Web and 24x7 availability of Internet to almost "everybody", the ethical concern regarding the widespread use of information technology is growing day by day. Today, people like to be parallel with the advanced technologies and have adopted Internet as an integral part of their life. In this regard, the need to manipulate technology in a way to use information correctly and realize information flow effectively is becoming essential (Moor, 2004). Even though various Information Technology innovations and tools have many advantages, if properly used but can also prove to be detrimental if abused. Cyber slacking (Greengard, 2002), fraudulence, sniffing, hacking, plagiarism, falsification (Mohamed, 2012) are some of the forms of computer abuse. These forms can serve as grounds for several societal and ethical problems varying according to the contexts and purposes of ICT use. Privacy and confidentiality of personal information in the virtual environment, integrity of the information used, intellectual property rights and access rights are just a few of the growing problems to name. The people using ICT need to be aware of the various ethical issues related to these problems so that equality and justice with regard to access, storage and distribution of information can be maintained (Charlesworth, 2000). There a need to invoke awareness among the users in regards to the ethical issue of human misuse and abuse of technology.

Ethics are often confused with etiquettes, skills, knowledge or manners that are essential for any job (Alexandra & Miller, 2010). But, in practice ethics relate to the question of right and wrong in human conduct (Benn, 1998; Kizza, 2003). This definition of ethics is in respect of general human behaviour in various aspects of life but the same definition can also be applied to meet the constantly changing technology-driven scenario of human conduct. Zeid (2009) stated that 'computer ethics deals with how to make moral decisions while using technology whether in workplace or in society in general'. Rogerson (1997), Goessl (2008) and Lee & Chan (2008) also insisted that the social and ethical implications of technology demand special attention and the attitude towards issues like free speech,

privacy, anonymity, copyright, etc. need to be revisited. Further, with the ever growing complexity of software systems, no single person can be expected to foresee and control the effects, especially the unwanted effects that technology might have on society. The incidents relating to the problems created by the inappropriate usage of technology like hacking, spoofing, cyber crimes, pornography, etc are increasing day by day. The onus for maintaining a standard protocol in the virtual environment lies with one and all. This has paved the path to a new concept that is often referred as "Cyber ethics", "Cyber Laws", "IT Ethics", "Internet ethics" or Information ethics". The aim of this article is to highlight some of the issues related to cyber ethics.

2. What is cyber Ethics?

Computer technologies and knowledge has transformed society and this transformation has urged a need that should indicate how various participants of the virtual environment must behave and regulate. Cyber ethics has been developed since the 1980s, encompassing areas such as computer ethics and global information ethics. As the name implies, cyber ethics is closely related to the use of computers by humans. James Moor in 1985 dealt with 'computer ethics' for the first time in his article 'What is Computer Ethics?'. He related computer ethics as having two parts, one that is related to the analysis of the nature and social impact of computer technology and the other with the corresponding formulation and justification of policies for the ethical use of such technology. He insisted that as human beings have to deal with moral decisions both as individuals and as a society, similarly computer ethics also involves the ethical use of information at both personal and social front. Moor (1988) Richard Spinello (2003) stated cyber ethics as a guide that suggests ways for ''acting well in this new realm of cyberspace''. Hence, cyber ethics must involve principles of morality that can guide human action so as to maintain a sustainable, participatory global information society. There are various terms that are often used interchangeably to describe cyber ethics. Some of these are:

- *Computer ethics*: It is basically related to the ethical and social impact of computers and computer networks in the information society (Stamatellos, 2007; Tavani, 2007, Bynum, 2001). These are the standards adopted for computer usage signifying the prevention of copyright infringement, invasion of privacy, and circulation of objectionable material. It is a normal belief that computer ethics rely on moral principles that help a computer user to make the right decision or to act right, accordingly.
- *Cyber Ethics:* It is a system of standards prescribing morality and immorality in cyberspace, in order to preserve freedom of expression, intellectual property, and privacy.
- *Internet ethics:* This includes various issues related to usage of internet and finding their solutions.
- *Information ethics*: This signifies ethics in terms of information or an information-oriented society. It relates to laying down various standards for judging behaviour of an individual or a member of community and classifying these as moral or immoral.

The author of this paper feels that all the above stated terms signify human behaviour relating to the handling/mishandling information in the virtual world and can thus, be broadly coined under "Cyber Ethics". Hence, cyber ethics primarily focus on the following:

- a. Prescribe the do's and don'ts in information society.
- a. Provide due consideration on the various ethical problems introduced due to the development of information and communications technology.
- b. Emphasise the need of human interaction, experience and the transformation of the system and policy. This is because it appears as a reaction against the dysfunction of large amounts of information, especially, the disorder and chaos in cyberspace.
- c. Include both global and local disciplines.
- d. Promote action/behaviour of the participants as a sense of responsibility.
- e. Formulate various ethical theories that are useful in solving ethical problems in both direct and indirect ways.

3. Issues relating Cyber Ethics

Computers, today, form an integral part of our life. They have slowly crept maybe "unsupervised" in all our daily activities and hence have the ability to affect human life. If one does not seriously examine the ethical implications relating to this "unsupervised" technology, then it may result into much bigger issues in future. This technology is so competitively accepted that as Moor says, "When a new computer technology is ready for market, nobody asks about its ethical implications. They may come later if at all". Hence, it becomes all the more imperative to be aware of various ethical issues concerning technology and subsequently adopt relevant ethical practices and habits. It is important to emphasise that it is not necessary that whatever is unethical need to be also illegal. It is essential to differentiate between unethical and illegal action. An illegal action can be subjected to its desired outcome through proper legal course; however an unethical act may at times have many severe repercussions and still may go unpunished. This makes it all the more important for a cyber user to be aware of various issues relating to cyber ethics and adopt subsequent behaviour. Privacy, Security, Personal Intrusion, Morality, Social networking sites, Accuracy, Intellectual Property rights, Accessibility, Deception, Internet research ethics, Technology and social responsibility are the most cited ethical issues of the information age. Though, some of these issues have individually been considered, yet this paper is going to throw new light in a comprehensive manner. The author of this paper makes a modest attempt to concentrate only on three major issues pertaining to cyber ethics which she feels must be in consensus with the social norms. These issues relate to privacy, social networking sites and Internet research ethics.

3.1   Privacy related Issues

Collection and usage of personal information is hardly a new practice. From time unknown, people in business and politics have been collecting personal information to aid in their decisions. So, why in this era of information, there is much hype about privacy. This is because, the amount of personal information collected, the speed of exchange of this information, the duration of time that this information can be retained, and the kind of information that can be acquired because of technology has the capacity to create controversies in real world. It is our moral duty and responsibility to maintain the privacy and integrity of data regarding individuals. It is often seen that policy makers or other profit making organizations covet information even if acquiring it invades another's privacy as information is increasingly valuable. This increases the potential for disclosure of information leading to violation of the privacy of any individual and groups of people. It is essential to take necessary precautions to ensure the accuracy of data, as well as protecting it from unauthorized access or accidental disclosure to inappropriate individuals. Some of the ethical issues that the author wants to stress in regards to the user awareness of the use of ICT and its impact on the privacy of users in the cyber world include:

- There is a need to be aware of the fact that the main purpose of Internet surveys, polls, registrations, and all manner of enticing rewards that pop up on the screen of Internet users is typically to collect information about users. It is important for cyber users to understand that this information can be stored indefinitely in databases where it can be later accessed and potentially correlated with other sources of data about the user.

- Most of the organizations allow intercepting and reading the e-mail messages of the employees as one of their security measures. Though, it is technically possible to intercept the e-mail messages, yet this may poses an ethical problem that may relate to the private communication of an individual. Although such practices may safeguard companies from employee dishonesty, but they can also create extremely stressful working conditions.

- Today information is money and thus selling information is so profitable. With the huge amount of information available through the networks, companies have begun to yield from their existing databases that they already hold for their own purposes and starting selling that to expecting parties for revenue. People need to be aware of exactly what they are revealing and to whom and the necessity of the information sought, when giving out information, however inadvertently.

- *Data banking* is often conducted by various organizations/government to merge the databases from a variety of databases into one central database. The main issue include the fact that the user is unaware of the fact that his/her personal information is being integrated into a central database, that the user is also not aware of the purpose/s for which the assimilation is being carried out, or whether this integration might potentially harm him/her later.

- The nature of information technology makes it relatively easier to record and monitor user's information. Thus, it is easy to violate average user's reasonable expectation of privacy on the Internet. It is very common nowadays to record a user's "click stream" or "mouse droppings". This brings us to the fact that a person's actions on the Internet are observed and recorded.

- The use of plastic cards on the Internet especially the "frequent-shopper cards" offer certain issues. These cards contain a computer chip that keeps record of various items purchased along with a variety of personal information of the buyer (Branscomb, 1995). This information obtained from the card enables marketing companies to do targeted marketing to specific individuals because the buying habits as well as other personal information of people are known. This is also violating the privacy of the individual.

- Hackers and system operators are the two kinds of individuals that have access to personal information that might be kept in a networked computer. Hackers and system operators do not necessarily pose a threat to privacy rights unless they get malicious and advertently harm the individual.

3.2   Social Media related issues

Social Media is a comprehensive term that is used to describe social interactions among individuals or groups through a suite of Internet based technology tools. Some of the most popular, but not limited to, tools are internet forums, Twitter, Facebook, blogs, LinkedIn, webcasts, whatsapp, Instagram, etc. This media is slowly gaining popularity among its users because of its speed and potential coverage of global audience. These tools are either free or are available at a relatively low cost and do not much require users to have technical knowledge to use it. From the utilitarian view, these tools are ethical as they help to build relationship and create greater good for greater number of people through interactions. Some of the ethical issues that the user needs to be aware include:

- The amount of information available on these social networking sites (SNS) often raises concerns like the capacity of facial-recognition software to automatically identify persons in uploaded photos, the use of automatic 'opt-in' privacy controls, the use of 'cookies' to track online user activities, the use of location-based applications for illicit monitoring or stalking, etc.
- Sharing of photographs and videos is often a facility offered by such sites that is not only most popular and but consequently often most misused aspects of online social networking. However, one should understand that living in society is bounded by its norms and rules and people often lack an ethical consideration of what behaviours should be displayed on the Internet.
- The Internet has emerged as a very important medium for the expression of information and ideas. Often many Internet users do not censor their written contents when interacting through social media tools. A need has often been felt to whether there should be content control or censorship of information available on Internet maybe by government or service providers. Various forms of information like pornography and other obscene forms of speech, hate speech such as websites of fascist and racist organizations, speech that can cause harm or undermine the state, such as information as to how to build bombs, speech that violates privacy or confidentiality, and libellous and defamatory speech are often felt to be under the scanner of censorship.
- The faceless environment of Internet often allows for the use of anonymity and intentional misrepresentation of self. This increases the probability that many individuals will forgo the basic considerations of the ethics of their online behaviour.

- SNS often give users control over their own privacy settings. It is always advisable to check out the settings, configuration and privacy sections in order to limit accessibility to your information.
- Now-a-days blogs use authenticated commenting systems like IntenseDebate that allow users to make anonymous or unregistered comments which makes it easy for someone to impersonate on a SNS or in blog comments. This can at times play havoc to the person's image or identity.
- Third-party applications are easily available that provide entertainment or other functionalities. One should avoid those applications that seem suspicious, and always modify the SNS settings to limit the amount of information the applications can access.
- It is always advisable to install software updates as and when they come so that attackers are unable to take advantage of known problems or vulnerabilities.

Questions are often raised that although there are extensive consequences of online social media tools, yet it becomes difficult to introduce certain ethical standards that will adequately address problems without being too restrictive of the freedoms that make the Internet so unique and popular. Instead, the onus must rely on the Internet users to apply the same societal parameters that exist in real world. It is always better to first evaluate the possible outcomes of any online activity and then accordingly set self imposed restrictions. This is merely a cautious perspective on the issue that ascertains the fact that it is better to be safe than sorry.

3.3   Internet research related issues

Internet research ethics (IRE) is an emerging interdisciplinary field that aims at studying the ethical implications that arise from the use of the Internet as a space and/or tool for research. It is an ethical priority of always respecting human beings as autonomous beings and thereby requires a number of rights, duties, and obligations in the form of rights to privacy, confidentiality, anonymity, and informed consent. Researchers thence have the obligation to respect and protect these rights, regardless of the "costs" of doing so, for example, of having to develop comparatively more complicated and/or costly research design to protect such rights, or even the ultimate cost of giving up an otherwise compelling and potentially highly beneficial research project because it unavoidably violates these basic rights and duties. In the virtual world, Plagiarism is the most common issue. It pertains to improperly using existing work either without authorization or without documentation. Researchers must respect the copyright issues and data ownership, and when permission should be sought to use potential data sources.

It is highly recommended to have respect for the autonomy and dignity of persons and thereby limit the extent to which potential data derived from online sources in the public domain. Many forums allow researchers to use material from open public domains freely without obtaining consent from the parties covered by the information. This must always be balanced against the requirement of respect for individuals' privacy and ownership. Researchers must follow the ethics relating to individual's choice and therefore remember that there may be a difference between what people view as private and what technically is publicly-available information about people's use, communication, production and interaction. Different participants on an Internet forum may have differing views of what is private and public, and their patterns of communication and behaviour will be influenced by this view. Researchers have special responsibility for safeguarding the research subjects' integrity. Researchers must not assume that all Internet users have a conscious view of or knowledge of which information will actually be made public and which information will not be made public.

Further, research projects that include persons must generally only be initiated after securing the subjects' free and informed consent. In other words, researchers must weigh relevant considerations and determine whether it is necessary to obtain consent or not. There is a distinction between researchers merely mining data and actively participating in a forum. If they actively participate in a forum with access restriction, researchers should present their intentions. Such disclosure should take place before starting the research. Similarly, there may also be reasons to make oneself known if information is obtained without active participation in the forum. Researchers must nevertheless take due consideration of ethical norms and any rules regarding behaviour that may apply to the forum.

Researchers are responsible for clearly explaining to research subjects their role and the expectations, limitations and requirements that pertain to their role as researcher

4. Conclusion

This paper has made a modest attempt to highlight the need for ethics in the cyber world particularly in the social networking sites, Internet related research and for privacy. But the core question is whether with the adoption of such information and communication technologies, should one simply also adopt new ethics? Expansionists like Carl Mitcham and Walter Maner argue that transformations made by ICTs on our society requires a new ethical framework, whereas traditionalists argue that the ordinary scheme of ethical analysis is also applicable to issues involving cyber technology (Tavani 2005, 2001). The author feels that both arguments are false and true. The information society is a societal formation that is both continuous and discontinuous, it is neither an entirely new society nor an entirely old society, but one based on asymmetrical distribution and accumulation of economic, political, cultural and information capital (Fuchs 2008). These structures have been transformed, though not revolutionized by the increasing usage of ICTs. Such partial change of society requires us to partly adapt our ethics.

The virtual world is full of stories on the one hand like cyberterrorism, information warfare, cyberhate, electronic surveillance, cybercrime, etc. and on the other hand like Wikipedia, social software, wikis, computer supported co-operative work, weblogs, online social networking, online friendships, digital democracy, file sharing, open source software, open content platforms, etc.. Both these phenomenon indicate different interplay of ethics in cyberspace. It, thus, lies on the users to adapt to the changes brought by ICT and make informed decisions to not only protect themselves but also within the realms of social welfare. It is also a duty for academicians to educate the youth of today regarding their responsible and ethical behaviour on the virtual world. The author feels that the academic institutions must initiate a cyber ethics curriculum both at the school and university level so that the youth is well versed with all the pros and cons of the new emerging IT world. By disseminating information and amending the curricula to address the ethical use of technology, the youth can be trained to become responsible cyber-citizens.

5. References

Alexandra, A., & Miller, S. (2010). Law, Ethics and Governance Series: Integrity Systems for Occupations. England: Asgate. pp: 61, and 113.

Ben-Jacob, M. G. (2005). Integrating Computer Ethics across the Curriculum: A Case Study. Educational Technology & Society, 8(4), 198 – 204.

Benn, P. (1998). Ethics. London: UCL Press.pp: 1-5.

Bynum T. W. and Rogerson, S. (1996). "Introduction and Overview: Global Information Ethics." Science and Engineering Ethics, 2/2: 131–6.

Charlesworth, M. (2000). How can a course in ethics and professionalism be included in an Information Systems Curriculum? A Research Project in the Department of Information Systems in the Faculty of Commerce of Rhodes University.

Goessl, L. (2008). How Computer Ethics Impact Society. Retrieved from http://www.helium.com/items/845336-how-computer-ethics-impact-society

Kizza, J. M. (2002). Ethical and social issues in the information age. New York: Springer Verlag.

Lee, W. W. & Chan, K. C. C. (2008). Computer Ethics: A Potent Weapon for Information Security Management. Retrieved from http://www.isaca.org/Journal/Past-Issues/2008/Volume-6/Documents/jpdf0806-computerethics.pdf

Moor, J. H. (2004). Reason, relativity and responsibility in computer ethics. T. W. Bynum, S. Rogerson eds. Computer Ethics and Professional Responsibility. Malden, MA: Blackwell Publishing.

Rogerson, S. (1997). Ethics and information technology. AJIS. 4 (2), 125 – 126.

Spinello, R.A. (1997). Case studies in Information and Computer Ethics, Prentice Hall, Upper Saddle River, NJ.

Tavani, H.T. (2004). Ethics and Technology, Ethical issues in an age of information and communication technology, John Wiley & Sons, New York.

Zeid, A. (2009). Using Creative Methods for Teaching Professional Ethics for Computer Science Students. First Kuwait Conference on E-Services and E-Systems on November 17-19. Retrieved from http://portal.acm.org/citation.cfm?id=1836047