Delhi Business Review ✍ Vol. 3, No. 1, January - June 2002

ETHICAL ISSUES IN CYBERAGE

Rajeev Kumra
R.K. Mittal

INTRODUCTION

Hacking as defined by Hacker.com is "the act of penetrating a closed computer system for the knowledge and information that is contained within it. Through the study of technology and computers a hacker can open his mind and expand his knowledge. Hacking should be intended to free information and expand minds and not to use it for destruction or material gain. There is always some debate as how the term hacker has been both glorified and undermined by the common media, but most will say that those who destroy data with illegal intent should be referred as crackers, not hackers'. There is need to look beyond this definition. What about the people's intellectual capital, which is impaired whenever, they loose their personal information without being compensated for it because of hacking? Hackers have often accessed or revealed privately intimate information of other users. The underlying ethical dilemma is of privacy vs. public control of information.

Today there are many such, ethical dilemma's related to cyberage such as – society's right to security vs. cryptography, freedom of speech vs. offensive information, private vs. public control of information. These issues are more relevant today, than at any other time. The millions of computers connected through each other have made the information accessible and approachable. This makes our society truly an information society and our time as cyberage. There are many unique ethical challenges, which stems from the nature of information itself.

The technological changes have outpaced ethical developments, thus bringing about unanticipated problem that have caused 'ethical vacuum'. The increasing number and variety of computer crimes committed by perfectly respectable and honest people shows the full limit of our understanding of computer ethics. Based on this reason, we have made an attempt to write this paper and highlight some of the ethical issues which society is confronting in this cyberage.We leave the final judgement on to the readers wisdom, moral standards and ethical framework to draw the logical conclusions out of this discussion.

Social Problems in Cyberage

Revolution in computer technology has affected our life in many ways, making this society a better place to live in. But, computer malfunctioning and its misuse has created many social problems and tensions associated with viruses, hacking, computer crimes, workplace privacy rights and adverse impact on kids. Let us probe these problems and issues in some detail.

Viruses

Every week there seems to be yet another story in press, outlining the horror of some new security threat involving E-mail or the Internet. Viruses, worms and Torjans, which are biggest threat to desktop security, have lately been found in lot of mailboxes. Earlier these viruses were passed on through demos of games on screen savers of discs, but now some viruses like 'melissa' can propagate themselves automatically, when the attachment is opened and can replicate without the attachment being accessed. Through this the whole organisation is paralyzed within no time. Torjans are mainly used for hacking into others machines. Torjans have the same rights as that of users (Govindarajan, 2001). So a remote hacker can delete or edit files, install software's or control peripherals. Recently, reputed Internet sites susceptible to what is called 'distributed denial of service' were attacked by the hackers using Torjans.

Hacking

Computer hacking is not a new phenomenon. Hacking only shows that doing e-damage does not require great weaponry but only some computer skills, which are not very difficult to acquire to make e-world unsafe. Even there are cases of school students (e-kids) penetrating highly sophisticated e-defenses and breaking into files of US military establishments. The purpose of hacking can range from simple sadistic pleasure to bad intention of cyber crime. It is one of the biggest social challenge, network managers have to face in the age of new information warfare.

Cyber Crimes

Concerns about cybercrime include; security of financial transactions, misuse of credit card information, guarding of proprietary of information exchanged during B2B or B2C transactions, privacy of e-mails and the invasion of personal privacy. Specifically companies that specialize in handling billing for the adult web site industry are increasingly the targets of cyber crooks looking to turn credit card number into cash (Asthana, 2001). Bad intentions of cyber criminals are a great concern for the society. Government is moving too slowly to tackle the rising tide of cyber crimes.

Work Place Privacy Rights

Employee privacy is considered as one of the most important social issue. Now employers have the capability to monitor their employees through electronic means. The question is do employers have the right to look at employee's E-mail and on the other hand do employees have a right of privacy that should prevent such an intrusion? Employers argue that they need the right to electronically monitor employees in order to enhance their job performance, prevent thefts, fraud and other illegal practices. They also argue that productivity, efficiency and quality control are enhanced by electronic surveillance. Is this a morally and ethically valid argument? On the other hand how much of right do employees have to use employers property as resource to pursue their own private goal. What about disgruntled employees who perform sensitive operations from within the security perimeter. They can take down system resources, alter data content and install backdoors for later use.

Adverse Impact on Kids

Recently Sushma Sawraj, I&B minister summoned Mr. Micheal adam, the CEO of FTV, to stop broadcasting nude fashion, as this create adverse impact on our culture and in particular on kids. This issue is of great concern in country like India. Now opening up a free adult websites is very much accessible for kids. Although age disclaimer is there on the sites but anybody can lie about his or her age and can access those sites. Impact on immature minds of kids is far reaching than fun, adventure or thrill. Internet makes them accessible to information, which can be harmful to their mental development, and they do not have a capability to distinguish between good and bad. Its impact is far reaching on culture and moral values.

The social problems enlisted above can be tackled fully or partially by many technology based solutions such as Intrusion Detection Systems ((IDS), Protocols, IPV6 (which allow network administrator to look at the hacker's source of address), screen saver passwords, encrypting the files, firewalls, virtual private networks and many more. Solutions based on technology to solve these social problems are insufficient. Simply because hackers or cyber criminals can always outsmart and can come up with unique methods of creating problems. Specifically issues like adverse impacts on kids and privacy of workplace cannot be fully solved by technology. For solving them we have to go deeper as their root lies in our society and individual ethics. The holistic solution is to find out the underlying ethical issues of these social problems.

Ethical Issues in Cyberage

Ethical issues involved in the above social problems are many and varied. However, it is useful and desirable to focus four most important issues relating to privacy, accuracy, intellectual property and access. These can be summarized by an acronym – PAPA.

Privacy

This is related with what information about one's self or ones association must a person reveal to others, under what conditions and with what safeguards. What things can people keep to themselves and not be

forced to reveal to others? Imagine, when a group of diverse files relating to a person and his or her activities are integrated into a single large database collection. You or I may have contributed information about ourselves freely to each of the separate databases but that by itself does not amount to giving consent to someone to merge the data, especially if that merger might reveal something about us (Ryder, 2001). What if, collection of information can reveal intimate details about a person and can thereby deprive the person of the opportunity to form certain professional and personal relationships? This is the ultimate cost of an invasion of privacy.

Consider a case, which occurred few years ago in florida, a perfect case study of intrusion in privacy. The Florida legislature believed that the state's building codes might be too stringent and that, as a result, the taxpayers were burdened by paying for buildings which were underutilized. Several studies were commissioned. In one study at the Tallahassee Community College, monitors were stationed at least one day a week in every bathroom. Every 15 seconds, the monitor observed the usage of the toilets, mirrors, sinks and other facilities and recorded them on a form! This data was subsequently entered into a database for further analysis. Of course, the students, faculty and staff complained bitterly.

Feeling that this was an invasion of their privacy and a violation of their rights, state official's respondent however said that the study would provide valuable information for policy making. In effect the State argues that the value of the information to the administrators was greater than any possible indignities suffered by the students and others. Soon the human right organisations joined the fray. At their insistence the study was stopped, but only after the state got the information it wanted.

Accuracy:

Misinformation has a way of fouling up peoples lives, especially when the party with the inaccurate information has an advantage in power and authority. Consider a plight of common middle class man who with his wife finally saved enough money to purchase a flat in Delhi. They, also take a long-term house loan from a bank. Every month this man walks to the bank's nearby branch religiously does a payment of Rs. 6000/- towards a house loan. He always got his deposit counterslip stamped and signed. This process goes on month after month for fifteen years. Suddenly he gets a notice from bank for non-payment of dues. This poor chap goes to the bank with his previous deposit slips duly signed. But then the main frame computer to front desk computer indicates that he has not paid the loan and amount is recoverable at the compounded interest by auctioning his flat, as documents of flat are pledged to bank against loan. This is enough to give gentleman a heart stroke. Every time we design information in database which might be used to make decisions. So, it is our responsibility to be vigilant in the pursuit of accuracy in information. Today, we are producing so much information about so many people and their activities that our exposure to problems of inaccuracy is enormous. And this growth in information also raises another issues. Who owns it?

Property

One of the most complex issues we face, as a society is the question of intellectual property rights. There are substantial economic and ethical concerns surrounding these rights; concerns revolving around the special attributes of information itself and the means by which it is transmitted. Any individual item of information can be extremely costly to produce in the first instance. Yet, once it is produced, that information has the illusive quality of being easy to reproduce and to share with others. Moreover, this replication can take place without destroying the original. This makes information hard to safeguard since, unlike tangible property, it becomes communicable and hard to keep it to one's self. It is even difficult to secure appropriate reimbursements when somebody else uses your information.

We currently have several imperfect institutions that try to protect intellectual property rights. Copyrights, patents, encryption, oaths of confidentiality, and such old fashioned values as trust worthiness and loyalty are the most commonly used protectors of our intellectual property. Problems however, still abound in this area. Let us focus on just one aspect: artificial intelligence and its expanding subfield of expert systems. In the field of artificial intelligence, practitioners of artificial intelligence proceed by extracting knowledge, and then implanting it into computer software, where it becomes capital in the economic sense. This process of "disseminating" knowledge from an individual, and subsequently "amending" it into machines transfers control of the property to those who own the hardware and software. Is this exchange of property warranted? Consider some of the most successful commercial artificial intelligence systems of the day.

Who owns, for example, the chemical knowledge contained in DYNDREL, the medical knowledge contained in MYCIN, or the geological knowledge contained in PROSPECTOR. How is the contributor of this knowledge to be compensated?

Access

One must have the intellectual skills to deal with information. These are skill such as reading, writing, reasoning, and calculating. This is a task for education. We are creating a large group of information poor people, who have no direct access to the more efficient computational technology and who have little training in its use.

Frequently, access to database is gained only by means of acquiring a terminal or personal computer. For example, if you want access to the New York Times Index through the Mead corporation service, you must first have access to a terminal integrated circuits, photoelectric cells, vacuum tubes and ferrite cores. These are among the technological yield of this scientific theory.

This means that the people, who wish to use this service, should possess several things. First, they should know that the database exists and how to use it. Second, they must have acquired the requisite technology to access it. And third, they must have capacity to pay the fees for the data. Many people cannot or choose not to pay it and hence are excluded from participating fully in our society. In effect, they become information "drop outs" and in the long run this will become the source of many social problems.

Conclusion

The important question, which out of the above discussion is how to deal with the ethical issues, Can we apply the same yardsticks of ethics to cyberethics? Probably not, as the underlying factors in case of human beings differs from computers when the same ethical standards are applied to them. Dealing with ethical issues in cyber age is full of complexities some of these are discussed below1:

(1) The virtual nature of the actions in question often makes it possible for them to remain completely undetected and to leave no perceptible effects behind.

(2) Computer technology distances one user from another and hence diminishes his sense of direct responsibility, for his computer mediated, computer controlled and computer generated actions. Thus actions and their effect are separated which makes moral sanctions less applicable.

(3) Depersonalization and increasing sense of the practical anonymity of actions / effects diffuses ethical responsibility in the user and thus the corresponding lack of perceived accountability.

(4) We are taught morality only about human interaction in real life or actions involving physical and tangible objects, not with virtual actions or objects (computer). The justification is that hacker do not understand the real implications of their behaviour, independently of their technical competence.

(5) Forecasting or aggregating the value of unethical consequences of an individual action is impossible in rapidly changing computer environment.

The conventional macroethical theories propounded by great thinkers (Aristotle, Mill or Kant) are not applicable in totality in this cyberage. Well, cyberthics is at too much of crossroads of technical matters, social problems, moral, legal & ethical issues and philosophical analyses has to be done by everyone to reach a decisive end.

References

Asthana, R.G.S. (2001) "E terrorism threatens E business", June 1-15, Vol. 5, No. 15, Computer World.

http://www.misq.org/archivist

Luciano, Floridi (1998) "Information Ethics: On the Philosophical Foundation of Computer Ethics", March 25-27, Fourth International Conference on Ethical Issues of IT, Netherland.

Rodney, Ryder D. (2001) "Of Secrets & Privacy", Aug 1-15, Computer Today.

Sekhan, Govindarajan (2001) "OF Wroms & Torjans", Jan., PC Quest, Cyber Media Publication.