Ethical Issues in Cyberspace and IT Society

Hary Gunarto
Ritsumeikan Asia Pacific University

ABSTRACT: Ethics is a branch of philosophy that deals with what is considered to be right or wrong. As information in cyberspace can be accessed globally, a research field of "computer ethics" is needed to examine what is right and wrong for Internet users can do, and what are the social impacts of Information Technology (IT) in general. Such research will underpin action that must be taken not only to harness the power of the IT itself, but also to survive its revolution.

It is especially important to understand security, privacy issues, and major negative impacts of IT on cyberspace. Although some technical approaches such as: encryption, digital ID, and firewall methods have been developed to overcome some of the problems, legal actions must also be enforced worldwide which will address a growing number of ethical problems resulting from the negative impacts of IT in our global society.

As data, information, and computer networks can be threatened by many internal and external hazards internationally, computer ethics should be the concern of everyone. Governments in every country, public policy makers, computer professionals, organizations and private citizens must all take an interest and make their contributions, so that this global information can be exploited in a socially and ethically sensitive way for our future benefit and applications.

1. INTRODUCTION

Ethics is a branch of philosophy that deals with what is considered to be right or wrong. Definitions of ethics have been widely proposed, such as “codes of morals of a particular profession”, “the standards of conduct of a given profession”, “agreement among people to do the right and to avoid wrong”. Webster’s Collegiate Dictionary defines ethics as “the discipline dealing with what is good and bad and with moral duty and obligation”. In more simple words, it is the study of what is right to do in a given situation, and what we ought to do.

It is important to note that what is unethical is not necessarily illegal. In our everyday life, many individuals and organizations faced with common ethical problems. For example, the issue of a company legally monitoring employees’ e-mail is very controversial issues. According to the American Civil Liberties Union, tens of millions of computer users are monitored, most without their knowledge, by their employers. Employees have limited protection against employers’ electronic surveillance. Although several legal challenges are now underway, the law appears to support employers’ rights to read electronic mail and other electronic documents of their employees. In this matter, the definitions of “right” and “wrong” are not clear. Also, the distinction between what is illegal and

what is unethical is not always obvious (Stephan, 2002).

With the advanced computer technology, it is important to understand computer ethics related to security, privacy issues, and major negative impacts of IT (Information Technology). Strategies must be developed which address a growing number of global ethical questions resulting from these negative impacts of IT in Cyberspace and IT society. Here are some of the questions that need to be addressed:

- What information about individual can be revealed to others?
- What information about individuals should be kept in databases, and how secure is the information in the computer systems?
- How should one handle data piracy on the computer networks?
- Who is allowed to access the data and information?
- How can safeguards be introduced to ensure that the information can be accessed only by the right person or organizations?

2. ETHICAL ISSUES IN COMPUTING

Information Technology (IT) has a central role in commerce, industry, government, medicine, education, entertainment and society at large. Its economic and social benefits hardly need explanation. But like any other technologies, IT also has problematic implications, and some negative impacts on our society. It poses and creates some problems related to ethics, and contains in general three main types of ethical issues: personal privacy, access right, and harmful actions. Let us look more closely at these issues, exploring in each case the ways in which they affect the public reactions to this technological change.

In terms of personal privacy, IT enables data exchange of information on a large scale from anybody, on any locations or parts of the world, at any times. In this situation, there is increased potential for disclosing information and violating the privacy of any individuals and groups of people due to its widespread disseminations worldwide. It is our challenge and responsibility to maintain the privacy and integrity of data regarding individuals. This also includes taking precautions to ensure the accuracy of data, as well as protecting it from unauthorized access or accidental disclosure to inappropriate individuals.

The second aspect of ethical issues in computing systems is access right. Due to the current popularity of international commerce on the Internet, the topic of computer security and access right has moved quickly from being a low priority for corporations and government agencies to a high priority. This interest has been heightened by computer break-ins at places like Los Alamos National Laboratories and NASA in the US. Many attempts of such illegal access to United States government and military computers by computer hackers have been widely reported. Without implementation of proper computer security policies and strategies, network connections on the Internet can't be made secure from illegal accesses.

In computer ethics, harmful action means injury or negative consequences, such as undesirable loss of

information, loss of property, property damage, or unwanted environmental impacts. This principle prohibits use of computing technology in ways that result in harm to any of users, the general public, employees, and employers. Harmful actions include intentional destruction or modification of files and programs leading to serious loss of resources or unnecessary expenditure of human resources such as the time and effort required to purge systems from "computer viruses." In the following tables, a survey of various activities on Internet indicates that illegal information nowadays is often reported. The data shows that the percentage of response from Japanese companies and organizations is quite significant (Kubo, 1999).

Table 1. Illegal Information on Internet

Type of information:	**Percentage of response:**
Fraudulent Information	79.5%
Violation of Privacy	73.1 %
False Rumors	59.3%
Obscene Information	59.0%
Libel Information	55.2%
Civil Rights Violation	48.5%
Gambling Information	10.4%

Table 2. Prejudicial Information

Type of information:	**Percentage of response:**
False Rumors	73.1%
Drug Information	71.3 %
Sex Information	66.4%
Violence Information	63.4%

So far, there has been relatively little investigation into the privacy and security issues relevant to these ethical problems in IT and Cyberspace. Beside the false contents of information on Internet, many people tried to access information that they don't have rights to do so. For this reason, computer developers have proposed and used intrusion-detection systems as basis of security systems designed to protect privacy. Typically, the intrusion-detection systems determine if a user is an intruder or a legitimate user, generally by way of various internal system profiles.

3. INTERNATIONAL EFFORTS ON LEGISLATIONS

The growing threat to individuals is beginning to claim attention in national and international community. In many countries around the world, existing laws are likely to be unenforceable against such crimes. This lack of legal

protection means that businesses and governments must rely solely on technical measures to protect themselves from those who would pose false information, from who steal, deny access to, or even destroy valuable information.

Self-protection is not sufficient to make cyberspace a safe place to conduct business. The rule of law must also be enforced. Countries where legal protections are inadequate will become increasingly less able to compete in the new economy. As cyber crime increasingly breaches national borders, nations perceived as havens run the risk of having their electronic messages blocked by the network. National governments should examine their current statutes to determine whether they are sufficient to combat such kinds of crimes (Chan and Camp, 2002).

Until now, only few nations have amended their laws to cover computer crimes that need to be addressed, as shown in Table 3. Other countries begin to implement some initiatives, and it is clear that a great deal of additional work and efforts are needed before organizations and individuals can be confident that cyber criminals will think twice before attacking valued systems and information.

Table 3. IT Legislations in Some Countries

Country	Year	Legislation	Contents
USA	1970	Freedom of Information Act	Permits individuals to access any information about themselves stored in the Federal Government Offices.
USA	1980	Privacy Protection Act	Provides protection of privacy in computerized and other documents.
USA	1987	Computer Security Act	Requires security of information regarding individuals.
USA	1997	Consumer Internet Privacy Protection Act	Requires prior written consent before a computer service can disclose subscriber's information.
USA	1997	Data Privacy Act	Limits the use of personally identifiable information and regulates "spamming".
Japan	2000	MITI Legislation for E-commerce	Legal Provisions for Electronic Signatures & Certification, and Foundation for Network-Based Social and Economic Activities
Canada	2000	Information Technology Act	Establish a legal framework for IT
Singapore	1999	Electronic Transactions Regulations	Govern the actions of certification authorities in Singapore
Australia	2000	NSW Electronic Transactions Act	Application of legal requirements to electronic communications
UK	1998	Data Protection Act	Data protection and Right of data access

New participating countries started generating principles to protect individuals from the potential invasion of privacy that data collection and retrieval poses. These countries have adopted guidelines as statutory law, in whole or in part. The OECD (Organization for Economic Cooperation and Development) in the US has specific guidelines pertaining to data privacy that directly affect those dealing with Internet data access in general, and those who use so-called "personal data" in particular.

4. ENCRYPTION TECHNOLOGY TO MINIMIZE HARMFUL ACTIONS ON INTERNET

In World War II, scrambled messages, written using a secret code, were common to prevent the enemy from intercepting battle instructions. Today on the Internet, these scrambled messages are quite popular as we protect our credit card numbers and private information from enemy hackers. A mathematical technique, called encryption, is used to scramble/encode a message into an unreadable format. The message's recipient decrypts, or decodes, the data using a key that converts it back into a readable form. Such encryption is widely used in online banking transactions, stock trading, Internet shopping, in ATMs, in point-of-sale machines, and in electronic business-to-business transactions. Data can be encrypted in a number of forms: web information transmissions, e-mail, files, transactions, etc.

On homepage data transmissions, encryption system commonly implemented to protect data is Secure Sockets Layer (SSL). This encryption can be easily identified by its web page address which starts with “https:” in place of usual “http:”. Another sign that SSL is being used is the presence of a gold lock on the status bar in Microsoft's Internet Explorer or the presence of a gold outline around the Security toolbar button's lock in Netscape.

Most popular algorithms to encrypt files and email messages are DES (Data Encryption Standard), RSA (Rivest Shamir and Adleman), and PGP (Pretty Good Privacy). Each employs key method to encrypt data, which requires the use of two keys, a public and a private key. To encrypt an email message, the sender encrypts the email using the receiver's public key, which is widely known and can be obtained from a company or Internet public-key server. The email message is then sent in a locked, unreadable format. The receiver uses his private key, which is confidential to everyone except the recipient, to decrypt the message.

Recently, new Advanced Encryption Standard (AES) has been adopted by the U.S. government. Developed by two Belgian cryptographers, the algorithm, called Rijndael, is designed to better safeguard government data than the older standard and works on multiple hardware and software platforms. This encryption method uses little memory and provides a defense against a number of data attacks. This new technique is particularly important when data passes through shared systems or insecure network segments where multiple people may have access to the information. In these situations, sensitive data--such as passwords--should be encrypted in order to protect it from unintended disclosure or modification.

Another data protection that is specific for e-mail messages is called “digital ID”. As more people send confidential information by e-mail, it is increasingly important to be sure that documents sent in e-mail are not forged, and to be certain that messages sent cannot be intercepted and read by anyone other than the intended recipient. By using "digital IDs" in MS Outlook Express, senders can prove their identity in electronic transactions in a way similar to showing driver's license when people cash a check.

Similar to encryption technique, digital ID is composed of a "public key," a "private key," and a "digital signature." When somebody digitally signs messages, he/she is adding digital signature and public key to the message. The combination of a digital signature and public key is called a "certificate." With Outlook Express,

senders can specify a certificate to be used by others to send encrypted messages to recipient.

For secure data transmissions on the Internet, both SSL and digital ID are commonly used to identify the legitimate identity of senders and receivers. Both techniques allow people to send/receive data in privacy, so that no body on the Internet is able to do eavesdropping. Furthermore, they can also be used to prevent any modification of transaction or message on the computer networks (Internet).

Another protection method against computer crimes is called firewalls. Internet firewall is essentially one or more systems that control access between computer networks. In this regard, the Internet is nothing more than collections of very large computer networks that need to be isolated one from another. The firewall serves two basic purposes: it controls access to the network from outside users, and it also controls the transfer of information from the inside network to outside world (Internet). The most important thing to remember about firewall is that it creates an access control policy for the organization.

5. SOME OF THE REMAINING ISSUES

Information Technology also concerns computer professionals who design and create information systems and devices. Recently, national and international organizations, such as the International Federation of Information Processors (IFIP), the Association for Computing Machinery (ACM), Institute of Electrical and Electronics Engineers (IEEE), the British Computer Society (BCS) and the Institute of Data Processing Management (IDPM), have recognized the need for new codes of ethics to inform and advise their members about relevant social and ethical issues.

In the US since 1992, the ACM has established a new policy on professional ethics. National accrediting bodies, like the Computer Sciences Accreditation Board and the Accreditation Board for Engineering Technology, now also require that accredited university curricula in the computing sciences include mandatory instruction in the social and ethical effects of information technology. As listed in Table 4, commitment to ethical professional conduct has been proposed so that every member of the ACM will follow (ACM , 1992).

Table 4. ACM Commitments on Ethics

No	Ethical conducts
1	Contribute to society and human being.
2	Avoid harm to others.
3	Be honest and trustworthy.
4	Be fair and take action not to discriminate.
5	Honor property rights including copyrights and patents.
6	Give proper credit for intellectual property.
7	Respect the privacy of others.
8	Honor confidentiality.

9 Contribute to society and human being.

In this regards, ethical problems are very important to be understood, realized, and solved legally or technically, not only in one or two countries, but worldwide, since the use of such computing technology will change everything in our life: where and how we work, learn, shop, vote, spend time, and live (Zhong, Liu, and Yao, 2002). As many governments and organizations formulate new strategies, it is probably also important to realize some related questions that may drive directly or indirectly some ethical issues in general sense. Such strategies should address a growing number of worldwide community issues, which may affect our lives, such as:

- How should society cope with resulting unemployment and underemployment worldwide?
- How should governments and businesses deal with possible exploitation of poor countries by wealthy countries and multinational conglomerates?
- How can society provide people with jobs that are interesting, fulfilling and challenging?
- How will education in cyberspace be planned, administered and financed?
- How can safeguards be introduced to ensure that the poor are not excluded from employment opportunities, education, shopping, entertainment and many more things on the global information net?

6. CONCLUDING REMARKS

The new world of information society with global networks and cyberspace will inevitably generate a wide variety of social, political, and ethical problems. Many problems related to human relationships and the community become apparent, when most human activities are carried on in cyberspace. Some basic ethical issues on the use of IT on global networks consist of personal privacy, data access rights, and harmful actions on the Internet. These basic issues have been solved partially using technological approaches, such as encryption technique, SSL, digital IDs and computer firewalls. Besides these protection technologies, legal laws are also needed in cyberspace to address hundreds of countries, which are incorporated into one global network. Guidelines and strategies should be implemented so that global information can be exploited in a socially and ethically sensitive way for our future benefit and applications. These and many more ethical issues urgently need the attention of governments, businesses, educational institutions, public and private individuals worldwide.

7. REFERENCES

ACM, 1992, *ACM Code of Ethics and Professional Conduct, Association of Computing Machinery,* USA, October 1992.

Chan, Serena and L. Jean Camp, 2002, *Law Enforcement Surveillance in the Network Society*,

IEEE Technology and Society, Volume 21, Number 2, page 22-30.

Kubo, Takeaki, 1999*, Internet Revolution & Japanese IT Industry*, Symposium on Development of Information Industry in the Asia-Pacific Region, 5-8 October 1999, Srilanka, page 21-93.

Stephan, Karl D, 2002, *Is Engineering Ethics Optional?,* IEEE Technology and Society, Volume 20, Number 4, page 6-12.

Zhong, Ning, Jiming Liu, and Yiju Yao, 2002, *In Search of the Wisdom Web*, IEEE Computer, IEEE, Volume 35, No. 11, page 27-31.