**Institute of Distance Learning, KNUST**

2008

**Template**

**For**

**Course Material**

**A 3-credit course outlay**

**KWAME NKRUMAH UNIVERSITY OF SCIENCE AND TECHNOLOGY, KUMASI**

INSTITUTE OF DISTANCE LEARNING

*(B. SC. IN INFORMATION TECHNOLOGY, II)*

BIT265 PROFESSIONAL AND LEGAL ISSUES IN INFORMATION TECHNOLOGY

**[Credit: Three**.**]**

Click here to enter text.

# *Publisher Information*

*© IDL, 2009*

*All rights reserved. No part of this book may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage and retrieval system, without the permission from the copyright holders.*

*For any information contact:*

Dean

Institute of Distance Learning

New Library Building

Kwame Nkrumah University of Science and Technology

Kumasi, Ghana

Phone: +233-51-60013

+233-51-61287

+233-51-60023

Fax: +233-51-60014

E-mail: idldean@kvcit.org

idloffice@kvcit.org

kvcit@idl-knust.edu.gh

kvcitavu@yahoo.ca

Web: www.idl-knust.edu.gh

www.kvcit.org

ISBN:

Editors:

Publisher notes to the Learners:

1. Icons: - the following icons have been used to give readers a quick access to where similar information may be found in the text of this course material. Writer may use them as and when necessary in their writing. Facilitator and learners should take note of them.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Icon #1  j0293844  Learning Objective | Icon #2  EL 1  Activity | Icon #3  j0299125  Assignments | Icon #4  j0299171  Information | Icon #5  ⎋  Summary |
| Icon #6  🕙  Time For Activity | Icon #7  🏋  Self Assessment | Icon #8  👪  Group Discussion | Icon #9  📚  Read | Icon #10  🗹  New Terms |
| Icon #11  🎖  Well Done | Icon #12  ELE 3  Note/Learning Tip | Icon #13  🖐  Pause | Icon #14  EL 2  Question | Icon #15  🖳  Online |

2. Guidelines for making use of learning support (virtual classroom, etc.)

This course material is also available online at the virtual classroom (v-classroom) Learning Management System. You may access it at www.kvcit.org

# *Course Writer*

Course writer(s):

Kwaku Agyepong Pabbi

BSc. Computer Science, MSc. Information Systems

Lecturer

Department of Computer Science

Course developer(s):

Kwaku Agyepong Pabbi

BSc. Computer Science, MSc. Information Systems

Lecturer

Department of Computer Science

# *Acknowledgement*

I wish to thank all colleagues of the Department of Computer Science for their invaluable contributions to this text in whatever form.

# *Course Introduction*

Globalization and digital convergence in the emerging knowledge society has raised complex ethical, legal and societal issues. We are faced with complex and difficult questions regarding the freedom of expression, access to information, the right to privacy, intellectual property rights, and cultural diversity. ICT is an instrumental need of all humans for the gathering of information and knowledge, and as such, should be guaranteed as a basic right to all human beings. All over the world, rights that are already legally recognised are daily being violated, whether in the name of economic advancement, political stability, religious causes, the campaign against terrorism, or for personal greed and interests. Violations of these rights have created new problems in human social systems, such as the digital divide, cybercrime, digital security and privacy concerns, all of which have affected people’s lives either directly or indirectly. Most of the issues raised by the ICT are new to our society, and social and political institutions are at a loss as to how to deal with them.

Most of the examples cited in the text regarding Information Technology ethical issues are drawn from examples from more industrialized countries. This is however not out of place since industrial countries are leaders in ICT. Less industrialized countries like Ghana could take advantage and benefit from the experiences of countries such as the United States, United Kingdom, Australia, etc, who have walked that same path, made mistakes and rectified the situation by enacting laws to combat the negative challenges that the introduction of Information Technology and Systems bring. This course seeks to position the student in a much better frame of mind to contribute effectively when discussing and finding solutions to these ethical problem emanating from the introduction of Information Technology.

**COURSE OBJECTIVES**

1. To understand the ethical and social issues of the information age.
2. To understand the scope of an organization's legal and ethical responsibilities as well as the IT professional’s responsibilities.
3. To discuss and appreciate the inclusion of ethical theories as a tool for ethical decision-making.
4. To describe the harmful effects of computer networking and security threats that computer users face.
5. To discuss ways in which Information Technology is threatening our privacy and briefly describe rules and laws being enacted to combat the threat
6. To examine various protection for intellectual property and recognize the various form of protections for proprietary software as well as the available alternative of open-source software.
7. To discuss liability issues concerning poor system quality as well as the effects of Information Technology on jobs and the workplace.

**COURSE OUTLINE**

* Unit 1: MORALITY, ETHICS AND LAW
* Unit 2: INCLUDING ETHICAL CONSIDERATIONS IN DECISION MAKING
* Unit 3: COMPUTER NETWORKING AND SECURITY
* Unit4: INFORMATION RIGHTS: PRIVACY AND FREEDOM IN AN INFORMATION SOCIETY
* Unit 5: INTELLECTUAL PROPERTY
* Unit 6: COMPUTER RELIABILITY, EMPLOYMENT & WORK

**COURSE STUDY GUIDE**

This provides a monthly/weekly schedule of progress of your learning.

|  |  |  |
| --- | --- | --- |
| **Week #** | **Unit/Session** | **FFFS/Practical/Exam/Quiz** |
| 1 | Unit 1/Session 1-1 & Session 2-1 | Self Assessment 1-1 & Self Assessment 2-1 |
| 2 | Unit 2/Session 1-2 & Session 2-2 | Self Assessment 1-2 & Self Assessment 2-2 |
| 3 | Unit 3/Session 1-3 & Session 2-3 | Self Assessment 1-3 & Self Assessment 2-3 |
| 4 | Unit 4/Session 1-4 & Session 2-4 | Self Assessment 1-4 & Self Assessment 2-4 |
| 5 | Unit 5/Session 1-5 & Session 2-5 | Self Assessment 1-5 & Self Assessment 2-5 |
| 6 | Unit 6/Session 1-6 & Session 2-6 | Self Assessment 1-6 & Self Assessment 2-6 |

**GRADING**

Continuous assessment: 30%

End of semester examination: 70%

**Resources**

Choose an item.

You will require the BIT265 Professional and Legal Issues in Information Technology course material and access to the Internet for this course.

To complete this course you would need to accomplish 36 hours and 3 credits

**REFERENCES**

REFERENCES

[1] K. Laudon, J. Laudon*. Essentials of Management Information Systems.* London: Prentice Hall, 2006.

[2] Michael Quinn. *Ethics for the Information Age.* Addison Wesley, 2006.

[3] B. K. Williams, S. C. Sawyer, S. Hutchinson. *Using Information Technology*. Irwin/McGraw-Hill*,* 1997.

[4] “How many on-line?”, *Nua Internet Surveys* 2003, [www.nua.com/suveys](http://www.nua.com/suveys).

[5] Jonathan Krim, “Spam’s Cost to Business Escalates”, [www.washingtonpost.com](http://www.washingtonpost.com), March 13, 2003

[6] Mike Mushgrove, “AOL Reports Decline in Spam in the Past Year.” [www.washingtonpost.com](http://www.washingtonpost.com). Dec 28, 2004.

[7] Associated Press. “Justice Uphold Use of Internet Filters in Public Libraries.” *NY-Times.com*, June 23, 2003.

[8] “College Crack Down on Viruses.” Associated Press, September 2003.

[9] R. Stair, G. Reynolds. *Principles of Information Systems: A Managerial Approach*, Thomson Course Technology, 2006.

[10] S. Hutchinson, S. Sawyer. *Computers, Communication, and Information: A User’s Introduction.* Irwin/McGraw-Hill*,* 1998.

[11] C. Sykes. *The End of Privacy*. St Martin’s Press, New York, NY, 1999.

[12] D. E. Sanger “Kodak Infringes on Polaroid Patents.” The New York Times, September 14, 1985.

[13] “New Targets for Copyright Enforcement: Organized Crime.” CNet News.com, March 13, 2003.

[14] *The Open Source Definition,* 2003. [www.opensource.org/doc/definition.php](http://www.opensource.org/doc/definition.php).

[15] “Software Error Return Patent Office Mail.” The New York Times, August 9, 1996.

[16] W. Martyn, “Japan Retailer Deluged with Orders for $25 eMacs,” Compute World, April 23, 2004.

**RECOMMENDED TEXTBOOKS**

*1. Ethics for the Information Age* by Michael J Quinn (Second Edition); Addison Wesley.

*2. Essentials of Management Information Systems by* Kenneth C. Laudon & Jane Price Laudon*;* Prentice Hall, 2006.

*3. Principles of Information Systems: A Managerial Approach* by Ralph Stair & George Reynolds; Thomson Course Technology, Seventh Edition.

# 

# *Table Of Contents*

[*Publisher Information* iii](#_Toc403132842)

[*Course Writer* v](#_Toc403132843)

[*Acknowledgement* vi](#_Toc403132844)

[*Course Introduction* vii](#_Toc403132845)

[*Table Of Contents* xi](#_Toc403132846)

[Unit 1 1](#_Toc403132847)

[Morality, Ethics and Law 1](#_Toc403132848)

[SESSION 1-1: Morality and Ethics IN THE INFORMATION Age 3](#_Toc403132849)

[1-1.1 What is Ethics? 3](#_Toc403132850)

[1-1.2 Virtue and Vices, and the importance or Integrity 3](#_Toc403132851)

[1-1.3 The Difference between Morals, Ethics and Laws 4](#_Toc403132852)

[1-1.4 Professionalism 5](#_Toc403132853)

[1-1.5 Codes of Ethics and Professional Organizations 7](#_Toc403132854)

[1-1.6 A Corporate Code of Ethics 9](#_Toc403132855)

[SESSION 2-1: LAW AND ETHICS IN THE INFORMATION AGE 10](#_Toc403132856)

[2-1.1 Organizational Liability and the Need for Counsel 10](#_Toc403132857)

[2-1.2 Policy Versus Law 11](#_Toc403132858)

[2-1.3 Types of Law 12](#_Toc403132859)

[2-1.4 Ethics in Information Technology 14](#_Toc403132860)

[UNIT2 16](#_Toc403132861)

[INCLUDING ETHICAL CONSIDERATIONS IN DECISION MAKING 16](#_Toc403132862)

[SESSION 1-2: ETHICAL SENARIOS 17](#_Toc403132863)

[1-2.1 Scenario 1 17](#_Toc403132864)

[1-2.2 Scenario 2 18](#_Toc403132865)

[1-2.3 Scenario 3 18](#_Toc403132866)

[SESSION 2-2 THE DECISION-MAKING PROCESS 20](#_Toc403132867)

[2-2.1 Developing a Problem Statement 21](#_Toc403132868)

[2-2.2 Identifying Alternatives 22](#_Toc403132869)

[2-2.3 Evaluating and Choosing an Alternative 22](#_Toc403132870)

[2-2.4 Implementing the Decision 23](#_Toc403132871)

[2-2.5 Evaluate the Results 23](#_Toc403132872)

[SESSION 3-2: OVERVIEW OF ETHICAL THEORIES 26](#_Toc403132873)

[3-2.1 Subjective Relativism 26](#_Toc403132874)

[3-2.2 Cultural Relativism 27](#_Toc403132875)

[3-2.3 Devine Command Theory 28](#_Toc403132876)

[3-2.4 Virtue Ethics 29](#_Toc403132877)

[3-2.5 Kantianism 30](#_Toc403132878)

[3-2.6 Act Utilitarianism 31](#_Toc403132879)

[3-2.7 Rule Utilitarianism 32](#_Toc403132880)

[3-2.8 Social Contract Theory 33](#_Toc403132881)

[Unit 3 38](#_Toc403132882)

[COMPUTER NETWORKING AND SECURITY 38](#_Toc403132883)

[SESSION 1-3: NETWORKING 40](#_Toc403132884)

[1-3.1 Email and Spam 40](#_Toc403132885)

[1-3.2 Fighting Spam 42](#_Toc403132886)

[1-3.3 The Internet 45](#_Toc403132887)

[1-3.4 Children and the Web 46](#_Toc403132888)

[1-3.5 Breaking Trust on the Internet 48](#_Toc403132889)

[SESSION 2-3: COMPUTER AND NETWORK SECURITY 50](#_Toc403132890)

[2-3.1 Viruses, Worms, and Trojan Horses 50](#_Toc403132891)

[2-3.2 Hackers 55](#_Toc403132892)

[2-3.3 Denial-of-Service Attacks 57](#_Toc403132893)

[Unit 4 62](#_Toc403132894)

[INFORMATION RIGHTS: PRIVACY AND FREEDOM IN AN INFORMATION SOCIETY 62](#_Toc403132895)

[SESSION 1-4: Philosophical Look at Privacy and the Electronic Trail 64](#_Toc403132896)

[1-4.1 Threats to Privacy 64](#_Toc403132897)

[1-4.2 Perspective on Privacy 67](#_Toc403132898)

[1-4.3 Disclosing Information 68](#_Toc403132899)

[1-4.4 Public Information 70](#_Toc403132900)

[1-4.5 Public record 73](#_Toc403132901)

[SESSION 2-4: OTHER PRIVACY CONCERNS & LAWS ON PRIVACY 77](#_Toc403132902)

[2-4.1 Identity Theft 77](#_Toc403132903)

[2-4.2 Encryption 79](#_Toc403132904)

[2-4.3 Rules And Laws on Privacy 80](#_Toc403132905)

[2-4.4 Some Suggested Solutions 83](#_Toc403132906)

[Unit 5 86](#_Toc403132907)

[INTELLECTUAL PROPERTY 86](#_Toc403132908)

[SESSION 1-5: Intellectual Property Rights 87](#_Toc403132909)

[1-5.1 What Is Intellectual Property? 87](#_Toc403132910)

[1-5.2 Benefits And Limits to Intellectual Property Protection 90](#_Toc403132911)

[1-5.3 Legal Protection for Intellectual Property 91](#_Toc403132912)

[1-5.4 Fair Use 95](#_Toc403132913)

[SESSION 2-5: PROTECTION FOR PROPRIETY SOFTWARE & OPEN SOURCE SOFTWARE 102](#_Toc403132914)

[2-5.1 Software Copyrights 102](#_Toc403132915)

[2-5.2 Software Patents 103](#_Toc403132916)

[2-5.3 Consequences of Proprietary Software 105](#_Toc403132917)

[2-5.4 Open-Source Definition 106](#_Toc403132918)

[2-5.5 Beneficial Consequences of Open-Source Software 107](#_Toc403132919)

[Unit 6 112](#_Toc403132920)

[COMPUTER RELIABILITY, EMPLOYMENT & WORK 112](#_Toc403132921)

[SESSION 1-6: Computer Reliability 114](#_Toc403132922)

[1-6.1 Accountability, Liability, And Control 114](#_Toc403132923)

[1-6.2 Data Quality And System Errors 115](#_Toc403132924)

[1-6.3 Poor Software Performance Due To Software Bugs And Errors. 116](#_Toc403132925)

[1-6.4 Software System Failures 117](#_Toc403132926)

[1-6.5 Data-Entry Or Data–Retrieval Errors 118](#_Toc403132927)

[SESSION 2-6: Employment, Work And Health Concerns 122](#_Toc403132928)

[2-6.1 Employment And Job Losses 122](#_Toc403132929)

[2-6.2 Work Place Changes 123](#_Toc403132930)

[2-6.3 Health Concerns 126](#_Toc403132931)

[2-6.4 Other Concerns 128](#_Toc403132932)

Unit 1

Morality, Ethics and Law

Introduction

As a future information technology professional, you must understand the scope of an organization's legal and ethical responsibilities. The information technology professional plays an important role in an organization's approach to managing liability for privacy, security and ethical risk. In the modern litigious societies of the world, sometimes laws are enforced in civil courts, where large damages can be awarded to plaintiffs who bring suits against organizations. Sometimes these damages are punitive-assessed as a deterrent. To minimize liability and reduce risks from electronic and physical threats, and to reduce all losses from legal action, information technology practitioners must thoroughly understand the current legal environment, stay current with laws and regulations, and watch for new and emerging issues. By educating the management and employees of an organization on their legal and ethical obligations and the proper use of information technology and information security, IT professionals can help keep an organization focused on its primary objectives.

The first session of this unit starts by taking a look at some of these issues which have heightened ethical concerns and forms the basis for the need for this text. The unit continues with the four Key technological trends that are responsible for these ethical stresses. Next, terms associated with the discussion of ethics in an Information Society are defined and explained using a model. The first part of this unit ends with Professional codes of conduct that professional associations and societies promulgate to regulate themselves in the general interest of society. In the second part, you learn about the ethical issues related to information security, and about several professional organizations with established codes of ethics.

In the second session, you learn about the legislation and regulations that affect the management of information in an organization.

|  |  |
| --- | --- |
| j0293844 | Learning Objectives  After reading this unit you should be able to:   1. Describe the functions of and relationships among laws, regulations, and professional organizations. 2. Differentiate between laws and ethics 3. Understand the role of an IT professional and what a Professional code of ethics entails 4. Differentiate between policy and law 5. Explain different kinds of law that may apply to the IT professional 6. Understand what kind of situations falls under the realm of ethical problems 7. Appreciate the ethical issues that Information Technology raises. |

Unit content

**Session 1-1: Morality and Ethics in the Information Age**

1-1.1 What is Ethics

1-1.2 Virtue and Vices, and importance of integrity

1-1.3 Difference between Morals, Ethics and Law

1-1.4 Professionalism

1-1.5 Codes of Ethics and Professional Organizations

1-1.6 A Corporate Code of Ethics

**Session 2-1: Law and Ethics in the Information Age**

2-1.1 Organizational Liability and the need for Council

2-1.2 Policy verses Law

2-1.3Types of Law

2-1.4 Ethics in Information Technology

SESSION 1-1: Morality and Ethics IN THE INFORMATION Age

# 1-1.1 What is Ethics?

A **society** is an association of people organized under a system of rules designed to advance the good of its members over time. Cooperation among individuals helps promote the common good. People in society however compete with each other however trivial or significant the competition may be.

Every society forms a set of rules that establishes the boundaries of generally accepted behaviour. These rules are often expressed in a statement about how people should behave, and the individual rules fit together to form the moral code by which a society lives. Unfortunately the different rules often cave contradictions, and people are sometimes uncertain about what rule to follow. For instance, if you witness a friend copy someone else’s answer while taking an exam, you might be caught in a conflict between loyalty to your friend and the value of telling the truth. Sometimes the rules do not seem to cover new situations, and an individual must determine how to apply existing rules or develop new ones. You might have to apply old rules to new situations. You may strongly support personal privacy, but do you think an organization should be prohibited from monitoring employees’ use of email and Internet services at the workplace?

The term morality refers to social conventions about right and wrong that are so widely shared they become the basis for an established consensus. However, individual views of what is moral may vary by age, cultural group, ethnic background, religion, life experiences, education, and gender. There is widespread agreement on the immorality of murder, theft, and arson, but other behaviours that are accepted in one culture might be unacceptable in another. Even within the same society, people can have strong disagreements over important moral issues. In the Ghana, United States, and many parts of the world, issues such as abortion, stem cell research, the death penalty, gun control and gay rights are continuously debated, and people on both sides of these debates feel that their arguments are on solid moral ground.

# 1-1.2 Virtue and Vices, and the importance or Integrity

As children grow they learn complicated tasks – such as walking, talking, swimming, riding a bike, dancing azonto, and writing the alphabet – that they perform out of habit for the rest of their lives. People also develop habits that make it easier to choose between what society considers good or bad. A virtue is a habit that inclines people to do what is acceptable, and a vice is a habit of unacceptable behaviour. Fairness, generosity, and loyalty are examples of virtues, while vanity, greed, envy and anger are considered vices. Peoples’ virtues and vices help define their personal value system – the complex system of moral values by which they live.

**The importance of Integrity.**

Your moral principles are statements of what you believe to be rules of right conduct. As a child, you may have been taught not to lie, cheat or steal. As an adult facing more complex decisions, you often reflect on your principles when you consider what to do in different situations. Is it okay to lie to protect someone’s feelings? Should you intervene with a fellow student who seems to have a drug dependency problem? Can you cut corners on a project to meet a tight deadline on a project?

A person who acts with integrity acts in accordance with a personal code of principles. One approach to acting with integrity – one of the cornerstones of ethical behaviour – is to extend to all people the same respect and consideration that you expect to receive from others. Unfortunately, consistency can be difficult to achieve, particularly when you are in situation that conflicts with you moral standards. For example, you might believe it is important to do as your employer requests while also believing that you should be fairly compensated for your work. Thus if your employer insists that you do not report the overtime hours that you have worked due to budget constraints, a moral conflict arises. You can do as your employer request or you can insist on being fairly compensated, but you cannot do both. In this situation you may be forced to compromise one of your principles and act with an apparent lack of integrity.

Another form of inconsistency emerges if you apply moral standards differently according to the situation or people involved. To be consistent and act with integrity, you must apply the same moral standards in all situations. For example you may consider it acceptable to tell a little white lie to spare a friend some pain or embarrassment, but would you lie to a customer about a business issue to avoid unpleasantness? Clearly, many ethical dilemmas are not as right versus wrong but involves choices between right versus right.

# 1-1.3 The Difference between Morals, Ethics and Laws

Morals are ones personal beliefs about right and wrong; the term ethics describes standards or codes of behaviour expected of an individual by a group (nation, organization, profession) of which an individual belongs. For example, the ethics of the law profession demands that defence attorneys defend an accused client to the best of their ability, even if they know that the client is guilty of the most heinous and morally objectionable crime one could imagine.

According to M. J. Quinn, **ethics** is the philosophical study of morality, a rational examination into people’s moral beliefs and behaviour. Ethics may also be defined as a set of moral values or principles that govern the conduct of an individual or group. Ethics refers to the principle of right and wrong that can be used by individuals as free moral agents to make choices to guide their behaviour. Consider the following analogy. Society is like a town full of people driving cars. Morality is the road network within the town. People ought to keep their car on the roads. Those who choose to “do ethics” may be in balloons floating above the town. From this perspective, an observer can evaluate individual roads (particular moral guidelines) as well as the quality of the entire road network (moral system).The observer can also judge whether individual drivers are staying on (acting morally) or taking shortcuts (acting immorally). Finally, the observer can propose and evaluate various ways of constructing road networks (alternative moral systems). While there may in fact be a definite answer regarding the best way to construct and operate a road network, it may be difficult for the observers to identify and agree upon this answer, because each observer has a different view point[2]

Law is a system of rules that tell us what we can and cannot do. Laws are enforced by a set of institutions (police, courts, law-making bodies e.g. parliament). Legal acts are acts that conform to the law. Moral acts conform to what an individual believes to be the right thing to do. Laws can proclaim an act as legal, although many people may consider the act as immoral – for example, abortion.

# 1-1.4 Professionalism

A professional is someone who belongs to a professional body. When groups of people claim to

be professionals, they take on special rights and obligations based on their special claims to knowledge, wisdom, and respect. When you graduate, and people begin to treat you as a professional because you hold a qualification in your field which has a professional body attached to it, people will expect you to have developed a certain level of expertise and to do things competently, be responsible, and trustworthy. Professional bodies are the guarantors of your professionalism relating to the responsibility and trust which can be placed on you.

Information Technology and Information Systems raise new ethical questions for both individuals and societies because they create opportunities for intense social change, threatening existing distribution of power, money, rights and obligations. Like other technologies, such as steam engines, electricity, telephones, and radio, IT can be used to achieve social progress, but it can also be used to commit crimes and threaten cherished social values. The development of IT will therefore produce benefits for many, and costs for others. In this situation, the question then is – What is the ethical and socially responsible course of action to take when confronted with a situation that seems to present ethical issues?

But how do professional bodies decide what acts are appropriate and inappropriate?

In an attempt to ensure that IT professionals conduct their profession in an ethically and socially responsible manner, various organizations and associations have developed codes of ethics otherwise known as Professional codes of conduct, to regulate and promote ethical behaviour in the use of Information Technology.

Your profession decides what actions are appropriate and inappropriate through:

 Codes of conduct, codes of practice and standards.

 Computer law.

 Ethical decision making.

**Professional Codes of Ethics**

Professional codes of conduct are promulgated by associations of professionals. These professional groups take responsibility for the partial regulation of their professions by determining entrance qualifications and competence. Codes of ethics are promises by the profession to regulate themselves in the general interest of society. In return, professionals seek to raise both the pay and the respect given their profession.

The British Computer Society code of conduct for example outlines what is expected as a level of professional conduct, professional integrity, that you as a professional pay due heed to the public interest, that you are faithful to your employer and professional field, it also governs your technical competence and impartiality.

A code of good practice refers to how competent you are. The British Computer Society code of practice insists that you pay due attention to the personal requirements of not just yourself or your clients but also those people who might be working for you. The code of practice outlines that you pay due heed to the organisation and management issues involved in your work, how you should undertake contract work and pay attention to privacy, security and integrity. The code of good practice covers system development, system implementation and elements of live systems.

# 

# 1-1.5 Codes of Ethics and Professional Organizations

A number of professional organizations have established codes of conduct or codes of ethics that members are expected to follow. Codes of ethics can have a positive effect on people's judgment regarding computer use. Unfortunately, many employers do not encourage their employees to join these professional organizations. But employees who have earned some level of certification or professional accreditation can be deterred from ethical lapses by the threat of loss of accreditation or certification due to a violation of a code of conduct. Loss of certification or accreditation can dramatically reduce marketability and earning power.

It is the responsibility of IT professionals to act ethically and according to the policies and procedures of their employers, their professional organizations, and the laws of society. It is likewise the organization's responsibility to develop, disseminate, and enforce its policies. Following is a brief discussion of some professional organizations and where they fit into the ethical landscape. Many of these organizations offer certification programs that require the applicants to subscribe formally to the ethical codes.

**Major IT Professional Organizations**

Many of the major IT professional organizations maintain their own codes of ethics.

**The Association of Computing Machinery (ACM)** (www.acm.org) is a respected professional society that was established in 1947 as "the world's first educational and scientific computing society." It is one of the few organizations that strongly promotes education and provides discounts for student members. The ACM's code of ethics requires members to perform their duties in a manner befitting an ethical computing professional. The code contains specific references to protecting the confidentiality of information, causing no harm (with specific references to viruses), protecting the privacy of others, and respecting the intellectual property and copyrights of others. The ACM also publishes a wide variety of professional computing publications, including the highly regarded Communications of the ACM.

**The International Information Systems Security Certification Consortium, Inc**. (ISC) (www.isc2.org) is a non-profit organization that focuses on the development and implementation of information security certifications and credentials. The (ISC)2 manages a body of knowledge on information security and administers and evaluates examinations for information security certifications. The code of ethics put forth by (ISC) is primarily designed for information security professionals who have earned an (ISC) certification, and has four mandatory canons: "Protect society, the commonwealth, and the infrastructure; act honourably, honestly, justly, responsibly, and legally; provide diligent and competent service to principals; and advance and protect the profession. This code enables (ISC) to promote reliance on the ethicality and trustworthiness of the information IT professional as the guardian of information and systems.

**The System Administration, Networking, and Security Institute (SANS)** (www.sans.org), which was founded in 1989, is a professional research and education cooperative organization with a current membership of more than 156,000 security professionals, auditors, system administrators, and network administrators. SANS offers a set of certifications called the Global Information Assurance Certification, or GIAC. All GIAC-certified professionals are required to acknowledge that certification and the privileges that come from it carry a corresponding obligation to uphold the GIAC Code of Ethics. Those certificate holders that do not conform to this code face punishment, and may lose GIAC certification.

Others are the **Information Systems Audit and Control Association (ISACA)** (www.isaca.org)which is a professional association that focuses on auditing, control, and security. The membership comprises both technical and managerial professionals.

The Information Systems Security Association (ISSA) (www.issa.org) is a non-profit society of information security professionals. As a professional association, its primary mission is to bring together qualified information security practitioners for information exchange and educational development

**The Ghana Institute of Information Technology(GIIT)** is the professional body of IT and computer professionals in the country. The Institute was registered on 4th October 1999, gazetted on 5th November 1999 and subsequently inaugurated on 2nd December 1999. Its membership includes world class professionals in the many diverse fields of Information and Communication Technology (ICT). They seek to set standards and influence education and training in information technology, data communication, etc.

The Institute has the following objectives among others:· To :-

* Foster networking among the members of the institute·
* Provide activities that will help one to improve his professional career.
* Provide technical information & services to computer professionals·
* Form a link between industries and education institutions in the country to set appropriate syllabi·
* Set Computing and Information technology standards for the information technology operations in the industries.
* Give free professional advice to organizations which finds themselves at the crossroads between their computing staff and service providers·
* Give free professional and impartial advice to government.

# 1-1.6 A Corporate Code of Ethics

A corporate code of ethics is a statement that highlights an organization’s ethical issues and identifies the overarching values and principles that are important to the organization and its decision making. Codes frequently include a set of formal, written statements about the purpose off an organization, its values, and the principles that should guide it s employees’ actions. An organization’s code of ethics applies to its directors, officers, and employees, and it should focus employees on areas of ethics risk relating to their role in the organization, offer guidance to help them recognize and deal with ethical issues, and provide mechanisms for reporting unethical conduct and fostering a culture of honesty and accountability within the organization. An effective corporate code of ethics helps ensure that employees abide by the law, follow necessary regulations, and behave in an ethical manner.

SESSION 2-1: LAW AND ETHICS IN THE INFORMATION AGE

Introduction:

In general, people elect to trade some aspects of personal freedom for social order. As Jean­Jacques Rousseau explains in The Social Contract, or Principles of Political Right, the rules the members of a society create to balance the individual rights to self-determination against the needs of the society as a whole are called laws. Laws are rules that mandate or prohibit certain behaviour; they are drawn from ethics, which define socially acceptable behaviours. The key difference between laws and ethics is that laws carry the authority of a governing body, and ethics do not. Ethics in turn are based on cultural mores: the fixed moral attitudes or customs of a particular group. Some ethical standards are universal. For example, murder, theft, assault, and arson are actions that deviate from ethical and legal codes throughout the world.

# 2-1.1 Organizational Liability and the Need for Counsel

What if an organization does not demand or even encourage strong ethical behaviour from its employees? What if an organization does not behave ethically? Even if there is no breach of criminal law, there can still be liability. Liability is the legal obligation of an entity that extends beyond criminal or contract law; it includes the legal obligation to make restitution, or to compensate for wrongs committed. The bottom line is that if an employee, acting with or without the authorization of the employer, performs an illegal or unethical act that causes some degree of harm, the employer can be held financially liable for that action. An organization increases its liability if it refuses to take measures known as due care. Due care standards are met when an organization makes sure that every employee knows what is acceptable or unacceptable behavior, and knows the consequences of illegal or unethical actions. Due diligence requires that an organization make a valid effort to protect others and continually maintains this level of effort. Given the Internet's global reach, those who could be injured or wronged by an organization's employees could be anywhere in the world. Under the U.S. legal system, any court can assert its authority over an individual or organization if it can establish jurisdiction-that is, the court's right to hear a case if a wrong is committed in its territory or involves its citizenry. This is sometimes referred to as long arm jurisdiction-the long arm of the law extending across the country or around the world to draw an accused individual into its court systems. Trying a case in the injured party's home area is usually favourable to the injured party

# 2-1.2 Policy Versus Law

Within an organization, information technology professionals help maintain security via the establishment and enforcement of policies. These policies-guidelines that describe acceptable and unacceptable employee behaviours in the workplace-function as organizational laws, complete with penalties, judicial practices, and sanctions to require compliance. Because these policies function as laws, they must be crafted and implemented with the same care to ensure that they are complete, appropriate, and fairly applied to everyone in the workplace. The difference between a policy and a law, however, is that ignorance of a policy is an acceptable defence. Thus, for a policy to become enforceable, it must meet the following five criteria:

• Dissemination (distribution)-The organization must be able to demonstrate that the relevant policy has been made readily available for review by the employee. Common dissemination techniques include hard copy and electronic distribution.

• Review (reading)-The organization must be able to demonstrate that it disseminated the document in an intelligible form, including versions for illiterate, non-English reading, and reading-impaired employees. Common techniques include recordings of the policy in English and alternate languages.

• Comprehension (understanding)-The organization must be able to demonstrate that the employee understood the requirements and content of the policy. Common techniques include quizzes and other assessments.

• Compliance (agreement)-The organization must be able to demonstrate that the employee agreed to comply with the policy through act or affirmation. Common techniques include logon banners, which require a specific action (mouse click or keystroke) to acknowledge agreement, or a signed document clearly indicating the employee has read, understood, and agreed to comply with the policy.

• Uniform enforcement-The organization must be able to demonstrate that the policy has been uniformly enforced, regardless of employee status or assignment.

Only when all of these conditions are met can an organization penalize employees who violate the policy without fear of legal retribution.

# 

# 2-1.3 Types of Law

**Civil law** comprises a wide variety of laws that govern a nation or state and deal with the relationships and conflicts between organizational entities and people

**Criminal law** addresses activities and conduct harmful to society, and is actively enforced by the state.

Law can also be categorized as private or public.

**Private law** encompasses family law, commercial law, and labor law, and regulates the relationship between individuals and organizations.

**Public law** regulates the structure and administration of government agencies and their relationships with citizens, employees, and other governments. Public law includes criminal, administrative, and constitutional law.

**Computer law**

In most countries there is a considerable body of law that can apply to computer professionals –

Contract law.

Intellectual property law.

Data protection law.

Computer misuse law.

Computer evidence.

If you intend to set yourself up in business you should become familiar with contract law. The most important thing to point out is that the ownership of intellectual property of something you developed depends very much on your role when you developed it. The key phrase is *“I did it in the course of my employment”* – if you develop something in the course of your employment the ownership generally belongs to your employer. If you do something as a contractor, invariably the ownership belongs to you – you have not been employed; you have been brought in and contracted to develop something.

If you are producing computer software with the intent of licensing the software to whoever commissioned it then you own the software. If you produce a piece of bespoke software then, unless you explicitly state in the contract that you intend to license the software, whoever commissioned it has paid you for, and therefore owns, what you have developed.

Contractual duties which you cannot avoid are:

Fidelity – dealing honestly and faithfully with people.

Confidence – how you respect the confidences that are given to you.

Culpability – the fact that you could be taken to court if you are negligent.

You CANNOT contract out of reasonable liabilities.

Intellectual property law centres on two main moral rights. The right of paternity, the right to be recognised as the person who created something. And the right of integrity, the right not to have your work tampered with by someone else. Copyright protects original works, sound recordings, and typographical layouts. Copyright lasts for 70 years after the death of the person who created it. In the case of a computer generated work, where the author cannot die, copyright expires 50 years after the work’s creation.

Patents protect work for 20 years. Patented ideas are generally novel and not obvious; the important thing to remember is that if you patent something you are expected to use it. In the UK a design right for designs such as printed circuit board layouts is recognised. There will be more on intellectual property later.

There are many statutes of data protection law; because of this it is difficult to distil general principles from these many statutes. The most important thing to remember is that the subject of personal data has the right to view and correct that data. Personal data should be accurate, adequate – sufficient for its purpose, relevant, and kept up to date. Personal data should not be kept for any longer than is necessary. All appropriate technical and organisational measures should be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of personal data. For computer data you should make sure that:

You have appropriate backups of the data.

You take appropriate security measures to secure the data.

There is more on privacy too.

Computer misuse law refers to unauthorised access and unauthorised modification. Unauthorised access of systems, programs, and data is unacceptable while unauthorised modifications through editing and deleting are forbidden. It has been recognised that, through the use of computers, it is possible to commit a crime in a country without actually being present in that country. Modern legislation can now state that it is irrelevant if you are in the country where the crime took place as long as it can be proved that you were responsible for the crime.

Computer evidence concerns what evidence is permissible in a court of law. Evidence may be invalidated if it is viewed after the event. An example of this is if you view log files with an editor after an intrusion, this will invalidate the logs as evidence as it is deemed that they might have been altered after the intrusion. Under normal circumstances specialists are brought in to follow audit trails back to the place of the attack. Amateurs could invalidate evidence or unwittingly tip off perpetrators.

# 2-1.4 Ethics in Information Technology

The growth of the Internet, the ability to capture and store vast amounts of personal data, and greater reliance on information systems in all aspects of life have increased the risk that information technology will be used unethically. In the midst of the many IT breakthroughs in recent years, the importance of ethics and human values has been underemphasized with a range of consequences. Here are some examples that raise public concern about the ethical use of information technology:

The great power of **email** is that it allows (at least in principle) anyone to send email to anyone else with an email address. Now that just about ‘everyone’ can have an email account, it is easier than ever to contact friends and family. Organizations contact millions of people worldwide through unsolicited email (spam) as an extremely low-cost marketing approach and about half of all email traffic is spam: unsolicited, bulk, commercial email. Is this alternative way of marketing spam destroying the value of email?

Thanks to the **World Wide Web**, it is easier than ever to share information with people all over the world. Imagine I live in America and post some files on my Web site. Some Ghanaians visit my web site and download the files, an action that violates Ghanaian laws. Should I be prevented from posting material that is legal in America but illegal in Ghana?

For many items of value, making the original copy is expensive, but making copies of the original is inexpensive. For example, a record company may spend hundreds of Ghana cedis to produce a CD, but copies can be burnt for just a few Ghana pesewas. Once CDs have been ripped into MP3 files, the internet provides a fast and efficient way to distribute them. • Millions of people have downloaded music and movies at no charge and in apparent violation of copyright laws at tremendous expense to the owners of those copyrights. As a result, **unauthorized copies** of song, movies, and computer programs are proliferating. Should we continue to give ownership rights to creators of intellectual property, or is it hopeless? If we no longer give ownership rights to creators of intellectual property, will creativity be stifled?

If I use a credit card to purchase an item, the credit card company now has information about my spending habits. Who has the **right to that information**? For example, if I buy boxes of bathroom tiles for my new house with my credit card, does the credit company have a right to sell my name, address, and telephone number to other companies that may want to sell other bathroom products?

The use of IT has changed the way that banks process loan applications in advanced countries. Rather than make a local decision regarding creditworthiness, banks can check a national credit bureau and ask for ones **credit rating**. What are the advantages and disadvantages of this alternative approach to lending money?

Computers are now embedded in many devices on which we depend, from traffic signals to pacemakers. **Software errors** have resulted in injury and even death. When bugs results in injury to human, what should the liability be for the people or corporation that produced the software?

When employees use IT devices in their work, companies can **monitor their actions closely**. For example, a company can track the number of calls per minute each of its telephone operators has handled. It can document the number of keystrokes per minute of its data entry operators. It can log all of the Web sites its employees visit. Many employees have their email and Internet access monitored while at work, as employers struggle to balance their need to manage important company assets and work time with employees’ desire for privacy and self direction. How does such monitoring affect the workplace? Does it create an unacceptable level of stress among employees or even infringements on their rights?.

**Hackers** break into databases of financial and retail institutions to steal customer information, then use it to commit identity theft—opening new accounts and charging purchases to unsuspecting victims.

Students around the world have been caught downloading material from the Web and **plagiarizing** content for their projects.

Web sites plant **cookies or spyware** on visitors’ hard drives to track their online purchases and activities.

IT is allowing more people than ever to **telecommute**; in other words, work from home. What are the advantages and disadvantages of telecommuting?

Finally, the World Wide Web has provided an unprecedented opportunity for individuals and governmental organizations to have their points of view made available to millions. This could bring about new levels of **citizen involvement and democratic reform**. On the other hand, some countries are making large portions of the Web unavailable to its citizens. Will the Web prove to be a tool for democracy, or will it be muzzled by repressive regimes?

These are all issues which the growth of IT has created and need to be addressed.

UNIT2

INCLUDING ETHICAL CONSIDERATIONS IN DECISION MAKING

Introduction

People who take the ethical point of view may still disagree over what is the proper course of action to take in a particular situation. Some disagreements are caused because people cannot agree on the facts of the matter. At other times, different value judgements lead people to opposite conclusions. Often the source of different value judgements is the use of different ethical theories to evaluate the problem. For this reason it is worthwhile to have a basic understanding of some of the most popular ethical theories. In this unit we will present some scenarios to give us an idea about ethical problems and try to take decisions on the situations. The steps of the decision-making process will be highlighted and a variety of ethical theories will be discussed.

|  |  |
| --- | --- |
| j0293844 | Learning Objectives  After reading this unit you should be able to:   1. Understand what class of problems or issues constitute ethical decision-making 2. Appreciate the steps that make up the decision-making process 3. Understand the principles of different ethical theories 4. Identify the case for and the case against an ethical theory 5. Decide when an ethical theory is workable 6. Analyze a situation based on the principles of a workable ethical theory |

Unit content

**Session 1-2:Ethical Scenarios**

1-2.1 Scenario 1

1-2.2 Scenario 2

1-2.3 Scenario3

**Session 2-2: The Decision-Making Process**

2-2.1 Developing a Problem Statement

2-2.2 Identifying Alternatives

2-2.3 Evaluating and Choosing an Alternative

2-2.4 Implementing a Decision

2-2.5 Evaluating the Result

**Session 3-2.1 Ethical Theories**

3-2.1 Subjective Relativism

3-2.2 Cultural Relativism

3-2.3 Devine Command Theory

3-2.4 Virtue Ethics

3-2.5 Kantianism

3-2.6 Act Utilitarianism

3-2.7 Rule Utilitarianism

3-2.8 Social Contract Theory

SESSION 1-2: ETHICAL SENARIOS

What do you do when you are confronted with a situation that seems to present an ethical dilemma?

To put us in a better frame of mind for the work at hand, let’s consider carefully, the following scenarios, curled from Michael J. Quinn’s book “Ethics for the Information Age”, and answer the questions that follow.

# 1-2.1 Scenario 1

An organization dedicated to reducing spam try to get Internet Service providers (ISPs) in an East Asian country to stop the spammers by protecting their mail servers. When this effort is unsuccessful, the anti-spam organization puts the address of the ISPs on its “blacklist”. Many ISPs in the United States consult the blacklist and refuse to accept email from the blacklisted ISPs. This action has two results. First, the amount of spam received by the typical email user in the United States drops by 25 percent. Second, tens of thousands of innocent computer users in the East Asian country are unable to send email to friends and business in the United States.

Questions

1. Did the anti-spam organization do anything wrong?
2. Did the ISPs that refused to accept email from the blacklisted ISPs do anything wrong?
3. Who benefited from the organization’s action?
4. Who was hurt by the organization’s action?
5. Could the organization have achieved its goal through a better course of action?

# 1-2.2 Scenario 2

In an attempt to deter speeders, the East Dakota State Police (EDSP) connects video cameras to all of its freeway overpasses. The cameras are connected to computers that can reliably detect cars travelling more than five miles per hour above the speed limit. These computers have sophisticated image recognition software that enables them to read license plate numbers and capture high resolution pictures of vehicle drivers. If the picture of the driver matches the driver’s license photo of one of the registered owners of the car, the system issues a speed ticket to the driver, complete with photo evidence. Six months after the system is put into operation, the number of people speeding on the East Dakota freeways is reduced by 90 percent.

The FBI asks the EDSP for real-time access to the information collected by the video cameras. The EDSP complies with this request. Three months later, the FBI uses this information to arrest five members of a terrorist organization.

Questions

1. Did the East Dakota State Police do anything wrong?
2. Who benefited from the action of the EDSP?
3. Who was harmed by the action of the EDSP? What other causes of action could the EDSP have taken to have achieved its objectives? Examine the advantages and disadvantages of these alternative courses of action.

# 1-2.3 Scenario 3

Joe works as a computer systems operator for a local police force in the city of Omaha. Doris, a patrol cop, calls into the station from her patrol car. She has just observed a driver that looks suspicious. Although the driver was not breaking the law, he was pressing the speed limit and seemed to be continuously looking over his shoulder. Though it was hard to tell from a distance, he appeared to be unkempt and unshaven. Doris took down his license plate number and is asking Joe to check the driver out on the system. Joe uses the license plate number and calls up the file on Willis Hawk. Hawk, aged twenty-five, was recently fired from his job at a local bakery. He is married, has two children under the age of five and lives in a middle-class Hispanic neighbourhood. Although he is in good standing with the local power and telephone companies and his credit card company, he is two payments behind on his mortgage. In the past five years Willis and his wife have attended several marriage counselling sessions. There is no record of Willis ever being arrested or convicted of a crime, but a year or so ago, the bakery that he worked for reported an internal theft and requested that Willis undergo a lie detector test. He was cleared. Joe conveys all of this information to Doris and she decides to follow Willis for a while longer.

Questions

1. Did Doris, the patrol cop, do anything wrong by asking Joe to check out Willis information?
2. Did Willis do anything wrong which must have called for such an investigation on him?
3. Can the information obtained on Willis be to his disadvantage? Racism for example?
4. Who benefits from such an action by the police?
5. Who is affected negatively by such an action by the police?
6. Are there any alternative causes of action the police could have taken to have achieved their objectives? What are these?

Now look back at the process you used to arrive at your answer. How did you arrive at your answer for each one of them, or decide if particular actions or decisions were right or wrong? Was your reasoning consistent? Did it not matter on which side you were on? If someone disagreed with you on the answer to any of these questions, would you be able to continence the person that your position makes more sense?

Ethics is the rational, systematic analysis of conduct that can cause benefit or harm to other people. Because ethics is based on reason, people are required to explain why they hold the opinion they do. This gives us the opportunity to compare ethical evaluations. When two people reach different conclusions, we can weigh the facts and the reasoning process behind their conclusions to determine the stronger line of thinking.

It is important to note that ethics is focused on the voluntary, moral choices people make because they have decided they ought to take one course of action rather than an alternative. Ethics is not concerned about involuntary choices or choices outside the moral realm.

SESSION 2-2 THE DECISION-MAKING PROCESS

We are all faced with difficult decisions in our work and in our personal life. Most of us have developed a decision-making process that we execute automatically, without thinking about the steps we go through. For many of us, the process generally follows the steps outlined in the Figure below

Develop Problem Statement

Identify alternatives

Evaluate and choose alternatives

Implement decision

Evaluate results

No

Success?

Yes

Finish

The following sections discuss this decision-making process further and point out where and how ethical considerations need to be brought into the process.

# 2-2.1 Developing a Problem Statement

A problem statement is a clear, concise description of the issue that needs to be addressed. A good problem statement answers the following questions: What do people observe that causes them to think there is a problem? Who is directly affected by the problem? Is there anyone else affected? How often does the problem occur? What is the impact of the problem? How serious is the problem? Development of a problem statement is the most critical step in the decision- making process. Without a clear statement of the problem or the decision to be made, it is useless to proceed. Obviously, if the problem is stated incorrectly, the decision will not solve the problem.

You must gather and analyze facts to develop a good problem statement. Seek information and opinions from a variety of people to broaden your frame of reference. During this process, you must be extremely careful not to make assumptions about the situation. Simple situations can sometimes turn into complex controversies because no one takes the time to gather the facts. For example, you might see your boss receive what appears to be an employment application from a job applicant and then throw the application into the trash after the applicant leaves. This would violate your organization’s policy to treat each applicant with respect and to maintain a record of all applications for one year. You could report your boss for failure to follow the policy, or you could take a moment to speak directly to your boss. You might be pleasantly surprised to find out that the situation was not as it appeared. Perhaps the “applicant” was actually a salesperson promoting a product for which your company had no use, and the “application” was marketing literature.

Part of developing a good problem statement involves identifying the stakeholders and their positions on the issue. Stakeholders often include others beyond those directly involved in an issue. Identifying the stakeholders helps you understand the impact of your decision and could help you make a better decision. Unfortunately, it may also cause you to lose sleep from wondering how you might affect the lives of others. However, by involving stakeholders in the decision, you can work to gain their support for the recommended course of action. What is at stake for each stakeholder? What does each stakeholder value, and what outcome does each stakeholder want? Do some stakeholders have a greater stake because they have special needs or because the organization has special obligations to them? To what degree should they be involved in the decision?

The following list includes one example of a good problem statement as well as two examples of poor problem statements:

• Good problem statement: Our product supply organization is continually running out of stock of finished products, creating an out-of-stock situation on over 15 percent of our customer orders, resulting in over ₵3,000,000 in lost sales per month.

• Poor problem statement: We need to implement a new inventory control system. (This is a possible solution, not a problem statement.)

• Poor problem statement: We have a problem with finished product inventory.(This is not specific enough.)

# 2-2.2 Identifying Alternatives

During this stage of decision making, it is ideal to enlist the help of others, including stakeholders, to identify several alternative solutions to the problem. Brainstorming with others will increase your chances of identifying a broad range of alternatives and determining the best solution. On the other hand, there may be times when it is inappropriate to involve others in solving a problem that you are not at liberty to discuss. In providing participants information about the problem to be solved, offer just the facts, without your opinion, so you don’t influence others to accept your solution.

During any brainstorming process, try not to be critical of ideas, as any negative criticism will tend to shut down the discussion, and the flow of ideas will dry up. Simply write down the ideas as they are suggested.

# 2-2.3 Evaluating and Choosing an Alternative

Once a set of alternatives has been identified, the group must evaluate them based on numerous criteria, such as effectiveness at addressing the issue, the extent of risk associated with each alternative, cost, and time to implement. An alternative that sounds attractive but that is not feasible will not help solve the problem.

As part of the evaluation process, weigh various laws, guidelines, and principles that may apply. You certainly do not want to violate a law that can lead to a fine or imprisonment for yourself or others. Are there any corporate policies or guidelines that apply?

Does the organizational code of ethics offer guidance? Do any of your own personal principles apply? Also consider the likely consequences of each alternative from several perspectives: What is the impact on you, your organization, other stakeholders (including your suppliers and customers), and the environment?

The alternative selected should be ethically and legally defensible; be consistent with the organization’s policies and code of ethics; take into account the impact on others; and, of course, provide a good solution to the problem.

Philosophers have developed many approaches to aid in ethical decision making. The most common approaches, which we refer to as ethical theories or principles are treated in the next session. They are;

* Subjective Relativism
* Cultural Relativism
* Divine command Theory
* Virtue Ethics Approach
* Kantianism
* Act Utilitarianism
* Rule Utilitarianism
* Social Contract Theory

These ethical theories provide a framework for decision makers to reflect on the acceptability of their actions and evaluate their moral judgments. People must find the appropriate balance among all applicable laws, corporate principles, and moral guidelines to help them make decisions.

# 2-2.4 Implementing the Decision

Once an alternative is selected, it should be implemented in an efficient, effective, and timely manner. This is often much easier said than done, because people tend to resist change. In fact, the bigger the change, the greater is the resistance to it. Communication is the key to helping people accept a change. It is imperative that someone whom the stakeholders trust and respect answer the following questions: Why are we doing this? What is wrong with the current way we do things? and What are the benefits of the new way for you? A transition plan must be defined to explain to people how they will move from the old way of doing things to the new way. It is essential that the transition be seen as relatively easy and pain free.

# 2-2.5 Evaluate the Results

After the solution to the problem has been implemented, monitor the results to see if the desired effect was achieved, and observe its impact on the organization and the various stakeholders. Were the success criteria fully met? Were there any unintended consequences? This evaluation may indicate that further refinements are needed. If so, return to the problem development step, refine the problem statement as necessary, and work through the process again.

🏋 **Self Assessment 1-1**

1. One who does ethics

1. examines people’s private lives
2. examines people’s moral beliefs and behaviour
3. is not concerned about involuntary choices
4. always follows the principle “Do unto others what you would have them do unto you”
5. I & II only
6. II & III only
7. II & IV only
8. I, II & III only
9. I & IV only

2. Professional Computer Societies include the

1. Association of Information Technology Professionals (AITP)
2. The Institute of Computer Scientists (ICS)
3. The Information Technology Association of America (ITAA)
4. Data Professionals for Social Responsibility (DPSR)
5. The Institute of Electrical and Electronic Engineers (IEEE)
6. I, II & III only
7. I, III & IV only
8. II & IV only
9. I, II, III & V only
10. I, III & V only

3. What are some of the reasons for which ethically minded people could disagree over what the proper courses of action to be taken in a particular situation are?

1. Disagreements on the facts of the matter.
2. Difference in their educational backgrounds.
3. Use of different value judgments (ethical theories).
4. I & II only
5. I & III only
6. II & III only
7. I only

e. II only

4. Rules of conduct that describe what people ought and ought not to do in various situations are called \_\_\_\_\_\_\_\_\_\_.

a. conditions

b. obligations

c. ethics

d. morality

e. constitution

SESSION 3-2: OVERVIEW OF ETHICAL THEORIES

Introduction

In the past two millennia, philosophers have proposed many ethical theories. We shall now briefly review some of them and take a look at the case for and against these ethical theories or principles. A useful theory is one that allows its proponents to examine moral problems, reach conclusions, and defend these conclusions in front of a sceptical, yet open-minded audience.

Ethical theories that are not based on reasoning or facts or commonly accepted values will be rejected. The workable theories are those that make it possible for a person to present a persuasive, logical argument to a diverse audience of sceptical, yet open-minded people.

In this unit we will discuss a variety of ethical theories, evaluate their pros and cons, and show how to use the more viable ethical theories to solve moral problems.

# 3-2.1 Subjective Relativism

Relativism is the theory that there are no universal moral norms of right and wrong. Different individuals and groups of people can have completely opposite views of a moral problem, and both can be right. Two particular kinds of relativism we shall discus are subjective relativism and cultural relativism.

Subjective relativism holds that each person decides right and wrong for himself or herself. This notion is captured in the popular expression “What’s right for you may not be right for me”.

**The Case for Subjective Relativism**

1. Well-meaning and intelligent people can have totally opposite opinions about moral issues.
2. Ethical debates are disagreeable and pointless.

**The Case against Subjective Relativism**

1. With subjective relativism the line between doing what you think is right and doing what you want to do is not sharply drawn.
2. By allowing each person to decide what is right and wrong for himself or herself, subjective relativism makes no moral distinction between the actions of different people.
3. Subjective relativism and tolerance are two different things.
4. We should not give legitimacy to an ethical theory that allows people to make decisions based on something other than reason.

If your goal is to persuade others that your solutions to actual moral problems are correct, subjective relativism is self-defeating. It is based on the idea that each person decides for himself or herself what is right and what is wrong. According to subjective relativism, no body’s conclusions are any more valid than anyone else’s, no matter how these conclusions are drawn. Because of its self defeating nature, we reject subjective relativism as a workable ethical theory.

# 3-2.2 Cultural Relativism

If subjective relativism is unworkable, how about different views of right and wrong held by different societies at the same point in time or those held by the same society at different points in time?

Cultural relativism is the ethical theory that the meaning of “right” and “wrong” rests with a society’s actual moral guidelines. These guidelines vary from place to place and from time to time.

Consider the following dilemma and how you think different societies will react.

You are driving in a car driven by a close friend. He hits a pedestrian. You know he was going at least 35 miles per hour. There are no witnesses other than you. His lawyer says that if you testify under oath that he was driving only 20 miles per hour, you will save him from serious consequences.

Different societies will answer differently to the following questions.

What right has your friend to expect you to protect him?

What do you think you would do in view of the obligations of a sworn witness and the obligation to your friend?

**The Case for Cultural Relativism**

1. Different social contexts demand different moral guidelines.
2. It is arrogant for one society to judge another.
3. Morality is reflected in actual behaviour.

**The Case against Cultural Relativism**

1. Just because two societies do have different views about right and wrong doesn’t imply that they ought to have different views.
2. Cultural relativism does not explain how an individual determines the moral guidelines of a particular society.
3. Cultural relativism does not do a good job of explaining how moral guidelines evolve.
4. Cultural relativism provides no framework for reconciliation between cultures in conflict.
5. The existence of many acceptable cultural practices does not imply that cultural practice would be acceptable.
6. Societies do, in fact, share certain core values.
7. Cultural relativism is only indirectly based on reason.

Cultural relativism has significant weaknesses as a tool for ethical persuasion. According to cultural relativism, the ethical evaluation of a moral problem made by a person in one society may be meaningless when applied to the same moral problem in another society. Cultural relativism suggests that there are no universal moral guidelines. It gives tradition more weight in ethical evaluations than facts and reason. For those reasons, cultural relativism is not a powerful tool for conducting ethical evaluations persuasive to a diverse audience.

# 3-2.3 Devine Command Theory

The three great religious traditions that arose in the Middle East – Judaism, Christianity and Islam – teach that a single God is the creator of the universe and that human beings are part of God’s creation. Each of these religions has sacred writings containing God’s revelation. If you are a religious person, living your life aligned with the will of God may be very important to you.

The Divine Command theory is based on the idea that good actions are those that align with the will of God and bad actions are those contrary to the will of God. Since the holy book contains God’s directions, we can use the holy book as moral decision-making guides. God says we should revere our mothers and fathers, so revering our parents is good. God says do no lie or steal, so lying and stealing are bad.

**The Case for Divine Theory**

1. We owe obedience to our creator.
2. God is all-good and all-knowing
3. God is the ultimate authority

**The Case against the Devine Command Theory**

1. There are many holy books and some of their teachings disagree with each other.
2. It is unrealistic to assume a multicultural society will adopt a religious-based morality.
3. Some moral problems are not addressed directly in scripture.
4. It is fallacious to equate “the good” with good.
5. The Divine Command Theory is based on obedience not reason.

The fact that moral guidelines are not the result of a logical progression from a set of underlying principles is a significant obstacle. While you may choose to align your personal actions with the divine will, divine command theory often fails to produce arguments that can persuade skeptical listeners whose religious beliefs are different. Hence we conclude the command divine theory is not a powerful weapon for ethical debate in a secular society.

# 3-2.4 Virtue Ethics

The virtue ethics approach to decision making focuses on how you should behave and think about relationships if you are concerned with your daily life in a community.

**The Case for Virtue Ethics**

1. It does not define a formula for ethical decision making, but suggests that when faced with a complex ethical dilemma, people do either what they are most comfortable doing or what they think a person they admire would do..
2. People are guided by their virtues to reach the “right” decision. A proponent of virtue ethics believes that a disposition to do the right thing is more effective than following a set of principles and rules, and that people should perform moral acts out of habit, not introspection
3. Virtue ethics can be applied to the business world by equating the virtues of a good businessperson with those of a good person.

However, businesspeople face situations that are peculiar to a business setting, so they may need to tailor their ethics accordingly. For example, honesty and openness when dealing with others are generally considered virtues; however, a corporate purchasing manager who is negotiating a multimillion dollar deal might need to be vague in discussions with potential suppliers.

**The Case against Virtue Ethics**

1. It doesn’t provide much of a guide for action.
2. The definition of virtue cannot be worked out objectively; it depends on the circumstances—you work it out as you go. For example, bravery is a great virtue in many circumstances, but in others it may be foolish.
3. The right thing to do in a situation also depends on which culture you’re in and what the cultural norm dictates.

# 3-2.5 Kantianism

Kantianism is the name given to the ethical theory of the German philosopher Immanuel Kant. Kant believed that people’s actions ought to be guided by moral laws, and that these moral laws were universal. He held that in order to apply to all rational beings, any supreme principle of morality must itself be based on reason. Hence while many of the moral laws Kant describes can be found in the Bible, Kant’s methodology allows these laws to be derived through a reasoning process. A Kantain is able to go beyond simply stating *that* an action is right or wrong by citing chapter and verse; a Kantain can explain *why* it is right or wrong.

**Kant’s Categorical Imperative.**

The moral value of any action depends on upon the underlying moral rule. It is critical, therefore, that we be able to determine if our actions are grounded in an appropriate moral rule. So what makes a moral rule appropriate? To enable us to answer this question, Kant proposes the Categorical Imperative which is as follows:

**“Act so that you always treat both yourself and other people as ends in themselves and never only as means to an end”**

To use popular terminology, this formulation of the Categorical Imperative which is the second, says it is wrong for one person to “use” another. Instead, every interaction with other people must respect them as rational beings.

Kantianism may also be referred to as the fairness approach because it focuses on how fairly actions and policies distribute benefits and burdens among people affected by the decision. The guiding principle of this approach is to treat all people the same. However, decisions made with this approach can be influenced by personal bias, without the decision makers even being aware of their bias. If the intended goal of an action or a policy is to provide benefits to a target group, other affected groups may consider the decision unfair.

**The Case for Kantainism**

1. Kantianism is rational.
2. Kantianism produces universal moral guidelines.
3. All persons are treated as moral equals.

**The Case against Kantainism**

1. Sometimes no single rule fully characteristics an action.
2. There is no way to resolve a conflict between rules.
3. Kantianism allows no exceptions to moral laws.

While these objections point out weaknesses with Kantianism, the theory does support moral decision-making based on logical reasoning from facts and commonly held values. It is culture neutral and treats all humans as equals. Hence it meets our criteria for a workable ethical theory, and we will use it as a way of evaluating moral problems.

# 3-2.6 Act Utilitarianism

**Principle of Utility**

The English philosophers Jeremy Bentham and John Stuart Mill proposed a theory that is in sharp contrast to Kantianism. According to Bentham and Mill, an action is good if it benefits someone; an action is bad if it harms someone. Their ethical theory, called utilitarianism, is based upon the Principle of Utility, also called the Greatest Happiness Principle. The utilitarian approach to ethical decision making states that you should choose the action or policy that has the best overall consequences for all people who are directly or indirectly affected. The goal is to find the single greatest good by balancing the interests of all affected parties.

The principle of utilitarianism is as follows:

**“An action is right (or wrong) to the extent that it increases (or decreases) the total happiness of the affected parties.”**

Utility is the tendency of an object to produce happiness or prevent unhappiness for an individual or a community. Depending on the circumstances, you may think of “happiness” as an advantage, benefit, good, or pleasure, and “unhappiness” as disadvantage, cost, evil, or pain. We can use the principle of Utility as a yardstick to judge all actions in the moral realm. We call utilitarianism a consequentialist theory, because the focus is on the consequence of an action.

Act utilitarianism is the ethical theory that an action is good if its net effect (over all affected **beings**) is to produce more happiness than unhappiness. It means, for example, that the environmental impact of decisions must often be included when performing the utilitarian calculus.

Utilitarianism fits easily with the concept of value in economics and the use of cost-benefit analysis in business. Business managers, legislators, and scientists weigh the benefits and harm of policies when deciding whether to invest resources in building a new plant in a foreign country, to enact a new law, or to approve a new prescription drug.

A complication of this approach is that measuring and comparing the values of certain benefits and costs is often difficult, if not impossible. How do you assign a value to human life or to a pristine wildlife environment? It can also be difficult to predict the full benefits and harm that result from a decision.

**The Case for Act Utilitarianism**

1. It focuses on happiness
2. It is down-to-earth
3. It is comprehensive

**The Case against Act Utilitarianism**

1. When performing the utilitarian calculus, it is not clear where to draw the line, yet where we draw the line can change the outcome of our evaluation.
2. It is not practical to put so much energy into every moral decision.
3. Act utilitarianism ignores our inmate sense of duty.
4. Act utilitarianism is susceptible to the problem of moral luck.

While it is not perfect, act utilitarianism is an objective, rational ethical theory that allows a person to explain why a particular action is right or wrong. It joins Kantianism on our list of workable ethical theories we can use to evaluate moral problems.

# 3-2.7 Rule Utilitarianism

**Basis of Rule Utilitarianism**

Rule Utilitarianism is the ethical theory that holds we ought to adopt those moral rules which, if followed by someone, will lead to the greatest increase in total happiness. Hence a Rule Utilitarian applies the principle of utility to moral rules, while an Act Utilitarianism applies the principle of utility to individual moral actions.

Both Rule Utilitarianism and Kantianism are focused on rules, and the rules these two ethical theories derive may have significant overlap. Both theories hold that rules should be followed without exception. However, the two ethical theories derive moral rules in completely different ways. A rule utilitarian chooses to follow a moral rule because its universal adoption would result in the greatest happiness. A Kantian follows a moral rule because it is in accord with the Categorical Imperative: all human beings are to be treated as ends in themselves, not merely as means to an end. In other words, the rule utilitarian is looking at the consequences of the action, while the Kantian is looking at the will motivating the action.

**The Case for Rule Utilitarianism**

1. Performing the utilitarian calculus is simple.
2. Not every decision requires performing the utilitarian calculus
3. Exceptional situations do not overthrow moral rules.
4. Rules utilitarianism solves the problem of moral luck.
5. It appeals to a wide cross of society.

**The Case against Rule Utilitarianism**

1. Utilitarianism forces us to use a single scale or measure to evaluate completely different kinds of consequences.
2. Utilitarianism ignores the problem of an unjust distribution of good consequences.

# 3-2.8 Social Contract Theory

According to philosopher Thomas Hobbes, without rules and a means of enforcing them, people would not bother to create anything of value, because nobody could be sure of keeping what they created. There would be social anarchy. To avoid this state of affairs, which Hobbes calls the “state of nature”, rational people understand that cooperation is essential. However, cooperation is possible only when people agree to follow certain guidelines. Hence moral rules are simply the rules that are necessary if we are to gain the benefits of social living. Hobbes argues that everybody living in civilized society has implicitly agreed two things: (1) the establishment of such a set of moral rules to govern relations among citizens, and (2) a government capable of enforcing these rules. He calls this arrangement **social contract**.

James Rachels summarizes these ideas in an elegant definition of social contract theory:

“*Morality consists in the set of rules, governing how people are to treat one another, that rational people will agree to accept, for their mutual benefit, on the condition that others follow those rules as well*”

The social contract theory to decision making is likened to the common good approach which is based on a vision of society as a community whose members work together to achieve a common set of values and goals. Decisions and policies that use this approach attempt to implement social systems, institutions, and environments that everyone depends on and that benefit all people. Examples include an effective education system, a safe and efficient transportation system, and accessible and affordable health care.

As with the other approaches to ethical decision making, there are complications with the common good approach. People clearly have different ideas about what constitutes the common good, which makes consensus difficult. In addition, maintaining the common good often requires some groups to bear greater costs than others—for instance, homeowners pay property taxes to support public schools, but apartment dwellers do not.

**The Case for Social Contract Theory**

1. It is framed in the language of rights
2. It explains why rational people act out of self-interest in the absence of a common agreement.
3. It provides a clear analysis of some important moral issues regarding the relationship between people and government.

**The Case against Social Contract Theory**

1. None of us signed the social contract.
2. Some actions can be characterized multiple ways.
3. Social contract theory does not explain how to solve a moral problem when the analysis reveals conflicting rights.
4. Social contract theory may be unjust to those people who are incapable of upholding their side of the contract.

🏋 **Self Assessment 1-2**

1. The notion behind \_\_\_\_\_\_\_\_\_\_\_ is captured in the popular expression “what is right for you may not be right for me.”

1. divine command theory
2. cultural relativism
3. subjective relativism
4. rule utilitarianism
5. social contract theory

2. \_\_\_\_\_\_\_\_\_\_\_ think ethical debates are disagreeable and pointless.

1. Kantians
2. Rule utilitarians
3. Act utilitatians
4. Divine command theorists
5. Subjective relativists

3. \_\_\_\_\_\_\_\_\_ think that it is arrogant for one society to judge another.

1. Moslems
2. Christians
3. Divine command theorist
4. Cultural relativists
5. Subjective relativists
6. I only
7. I & II only
8. I, II & III only
9. IV only
10. V only

4. Which ethical theory is based on obedience not on reason?

1. Kantianism
2. Act utilitarianism
3. Divine command theory
4. Rule utilitarianism
5. Social contract theory

5. \_\_\_\_\_\_\_\_\_\_ is the theory that holds that “right” and “wrong” rests with society’s actual moral guidelines.

1. divine command theory
2. cultural relativism
3. subjective relativism
4. rule utilitarianism
5. social contract theory

🏋 Self Assessment 2-2

1. Which ethical theory is based on “The greatest happiness principle?”

1. Act utilitarianism
2. Divine command theory
3. Rule utilitarianism
4. Social contract theory
5. Kantianism

2. \_\_\_\_\_\_\_\_\_\_\_ states that “take the action that achieves the higher of greater value”.

1. Social contract theory
2. Ethical ‘no free lunch’ rule
3. Divine command theory
4. Kant’s categorical imperative
5. Utilitarian principle

3. A \_\_\_\_\_\_\_\_\_ is able to go beyond simply stating that an action is right or wrong, but can explain why that action is right or wrong.

1. Kantian
2. Rule utilitarian
3. Subjective relativists
4. Act utilitarian

4. Which of these are considered consequentialist theories?

1. Rule utilitarianism
2. Act utilitarianism
3. Kantianism
4. Divine command theory
5. I only
6. II only
7. I & II only
8. I, II & III only
9. II & IV only

5. A \_\_\_\_\_\_\_\_\_\_\_ believes in many laws which can be found in the bible but are also backed by a reasoning process.

1. Christian
2. Divine command theorist
3. Kantian
4. Social contract theorist
5. Relativist

 *Learning Track Activities*

|  |  |
| --- | --- |
| j0299125 | **Unit Assignments 2**  1. What do we mean when we say an ethical theory is workable?  2. Give reasons why you may argue for or against the use of cultural relativism as an ethical theory for the drawing up of guidelines to resolve ethical problems emanating from the use of IT?  3. Give three (3) reasons why one may argue against Divine Command Theory as an ethical theory.  4. What arrangement does the philosopher Thomas Hobbs call a “social contract” and why is there a need for such an arrangement? |
|  |  |

Unit 3

COMPUTER NETWORKING AND SECURITY

Introduction

You can put an isolated computer to a lot of good uses-such as word process­ing, touching up digital photographs, constructing spreadsheets, and playing games - ­but a computer's utility increases tremendously when it is connected to a network. Net­worked computers can share resources such as printers or extra storage. Networks also support the exchange of email and files.

The Internet has greater value still, because it connects millions of computers. If your computer is connected to the Internet, you can send email to anyone else in the world that also has an email account. You can surf the World Wide Web's billion-plus pages for information, products, and services, or you can use the Web to promote your own company.

In this session we explore the moral issues associated with our use of the Internet. We begin by focusing on email, the most popular Internet application. We then discuss how spam, unsolicited bulk email, has degraded the quality of email service.

The World Wide Web has proven to be the most popular way of organizing information on the Internet and many governments and individuals find much of the information they find on the web to be subversive, dangerous, or immoral. We discuss inappropriate Web content and the different kinds of censorship next.

Next we focus on the issue of children and the Web and how the Internet provides new ways to commit fraud and deceive people using for example identity theft.

The utility of our computers and the information they hold makes computer security an important issue. The next session focuses on threats to computer security. We begin by surveying computer viruses, worms, and Trojan Horses. Through these mechanisms unauthorized programs can enter our computers. When executed, they can steal personal information, destroy data, and even launch attacks on other computers. System administrators play a key role in defending computers from outside threats. We review some of the ways administrators increase the security of the systems for which they are responsible.

Our focus then shifts from unauthorized programs to unauthorized people. People who use computers without authorization are called hackers. We look at the hacker culture of MIT in the 1950s and 1960s.

In the past few years, denial-of-service attacks have temporarily disabled Internet-based servers managed by many organizations. We end this section by examining some popular denial-of-service attack strategies and ways of combating them.

|  |  |
| --- | --- |
| j0293844 | Learning Objectives  After reading this unit you should be able to:   1. Understand how Email works 2. Gain an insight into strategies that spammers use 3. Describe ways being used to fight spam and suggest solutions to the spam epidemic 4. Describe whether there is too much control or too little control concerning the use of the Internet in your part of the world 5. Describe efforts being made to meet threats on the Web that children face 6. Appreciate ways fraudsters employ in obtaining personal information about unsuspecting victims of identity theft 7. Distinguish between viruses, worms, and Trojan houses 8. Explain defensive measures that can be employed to ensure system security 9. Describe the activities of Hackers 10. Identify different kinds of Denial-of-Service attacks 11. Employ a variety of defensive measures to reduce the threat of Denial-of-Service attacks |

Unit content

**Session 1-3: Networking**

1-3.1Email and Spam

1-3.2 Fighting Spam

1-3.3 The Internet

1-3.4 Children and the Web

1-3.5 Breaking Trust on the Internet

**Session 2-3: Computer and Network Security**

2-3.1 Viruses, Worms, and Trojan Horses

2-3.2 Hackers

2-3.3 Denial-of-Service Attack

SESSION 1-3: NETWORKING

# 1-3.1 Email and Spam

**How Email Works**

Email refers to messages embedded in files transferred from one computer to another via a telecommunications system. An email address uniquely indicates a virtual mailbox in cyberspace. Every email address has two parts. The first part (before the @ sign) identifies the individual user. The second part (after the @ sign) identifies the domain name. If you are a college student, your college may provide you with an email account, in which case some or your entire domain name is the domain name of your college. Another way to get an email account is through an Internet service provider (ISP). Each ISP has its own domain name.

Suppose you want to send an email to your friend Emmanuel Ofori Oppong (login name EOOP) at Kwame Nkrumah University of Science and Technology (domain name knust.edu.gh). You compose the message, indicate the recipient is EOOP@knust.edu.gh, and send the message. Your mail server uses the domain name system (DNS) to look up knust.edu.gh and find its Internet Protocol (IP) address. This address uniquely identifies a mail server at Kwame Nkrumah University of Science and Technology in Ghana. Next, if your email message to Emmanuel Ofori Oppong is more than a few lines long, it is broken up into two or more pieces, called *packets.* At the front of each packet is the IP address of Kwame Nkrumah University of Science and Technology, Ghana.

There is a good chance that your mail server is not directly connected to Emmanuel Ofori Oppong's mail server. The Internet contains thousands of interconnected routers that cooperate to get IP packets to their destination. Your server sends the packets to a router that is on the path to Kwame Nkrumah University of Science and Technology. It forwards the packets to the next router on the path, and so on, until the packets arrive at Emmanuel Ofori Oppong’s mail server. His mail server reassembles the packets into an email message and puts it in his mailbox.

**The Spam Epidemic**

The growth of email has been phenomenal. Surveys reveal that in September 2002 there were about 180 million people with access to email in the United States and Canada, and about 600 million worldwide [4]. Every day billions of email messages are exchanged. Unfortunately, a significant percentage of this traffic consists of unsolicited bulk email, or spam.

Dealing with spam has become one of the Internet's biggest problems. As recently as the year 2000, spam accounted for only about 8 percent of all email. Back in those days, it was viewed as a problem for individuals managing their mailboxes. By 2003, about 40 percent of all emails were spam[5]. Currently, spam consumes a large percentage of the Internet's bandwidth and huge amounts of storage space on mail servers and individual computers. The cost to businesses is estimated at billions of dollars per year in wasted productivity [2].

The volume of spam is increasing because companies have found it to be effective. The principal advantage of spam is its low cost compared to other forms of advertising. For between $500 and $2,000, a company can hire an Internet marketing firm to send an advertisement to a million different email addresses. Sending the same advertisement to a million addresses using the U.S. Postal Service costs at least $40,000 for the mailing list and $190,000 for bulk-rate postage. And that doesn't include the cost of the brochures! In other words, an email advertisement is more than 100 times cheaper than a traditional flyer sent out in the mail. The cost is so low that a company can make money even if only one in 100,000 recipients of the spam actually buys the product or service [2].

How do direct marketing firms build email lists with millions of addresses? One way a spammer can get your email address is through an opt-in list. Have you ever entered a contest on the Web? There is a good chance the fine print on the entry form said you agree to receive "occasional offers of products you might find valuable" from the company's marketing partners; in other words, spam. Sign-ups for email lists often contain this fine print, too.

Another way spammers get your email address is through so-called dictionary attacks. The term comes from programs that try to guess passwords by trying ev­ery entry in an online dictionary. In this case, it means spammers bombard Inter­net service providers with millions of emails with made-up email addresses, such as AdamA@isprovider.com, AdamB@isprovider.com; AdamC@isprovider.com; and so on. Of course, most of these emails will bounce back, because the addresses are no good. However, if an email *doesn't* bounce, the spammer knows there is a user with that email address and adds it to its mailing list.

To keep networks from being flooded with spam, ISPs have installed spam filters to block spam from reaching users' mailboxes. America Online's spam filters block more than *one billion* email messages a day [6]. These filters look for a large number of messages coming from the same email address, messages with suspicious subject lines, or messages with spam-like content.

Despite these measures, a tremendous amount of spam is still being delivered to email users. Spammers are changing their tactics to confound the efforts of spam blockers.

Spammers disguise themselves by changing email addresses and IP addresses to dis­guise the sending machine. Some innocent victims of "spam spoofing" have received tens of thousands of bounced-back emails. Others have lost their email privileges for violating their ISP's anti-spam policy. Unfortunately, spam spoofing is "easy to do, difficult to trace, and impossible to prevent".

Spam spoofing is when a spammer falsifies outgoing emails to make it appear that they originated from someone else. The innocent victim receives the email that bounces back due to an invalid address, as well as complaints from irate recipients of the spam.

Another trick used by spammers is to divert attention to an innocent bystander by using that person's system as the launch pad for a spam attack.

Spammers buy spam-screening software and check to see if their messages are blocked. If so, they modify their messages until they pass through the screens. Spam­mers have changed to more complicated (or more misleading) subject lines, such as "How are you?"; "Thanks for requesting more information"; and "Error in your favour."

Once screeners started checking the bodies of messages for key words, some spam­mers began switching to images containing the message. The introduction of explicit pornographic images in spam has infuriated many email users. It has also raised con­cerns that the appearance of pornographic images in people's mailboxes will lead to legal charges against companies for tolerating a work environment that is hostile to women.

# 1-3.2 Fighting Spam

**Mail Abuse Prevention System**

Mail Abuse Prevention System (MAPS) is a California-based not-for-profit organization dedicated to reducing the flow of spam through the Internet. MAPS maintains a Real­time Blackhole List (RBL), a list of networks that either forward spam or allow spam to be created, and it makes this list available to third parties. Network administrators can make use of the RBL to protect their mail relays from being used by spammers. When a mail relay receives an incoming mail message from an untrusted host, it can make a DNS query against the RBL. If the result of the query indicates the host is on the RBL, the mail relay can reject the email, bouncing it back to the sender.

How does MAPS decide if a network should be blacklisted? The organization has produced a set of guidelines it believes represent "best current practices" for sending bulk email. Here is a summary of the MAPS guidelines for organizations that manage mailing lists:

* They must be able to verify that the recipients of their messages have subscribed to their email lists. Potential subscribers verify their desire to receive marketing emails by replying to a verification message or visiting a Web site and filling in a form. Subscribers to one list should not be automatically added to another list.
* They must take care not to overwhelm individual hosts or LANs
* They must disclose to subscribers how their addresses will be used, including the frequency and subject matter of future mailings.
* They must provide subscribers with simple ways to terminate their subscriptions, including at least one non-email communication mechanism (such as a telephone number).
* They must remove invalid email addresses from their mailing lists in a timely manner.

When MAPS becomes aware of an email marketer violating these standards, it contacts the marketer (or its ISP) with a warning that it may be placed on the Realtime Blackhole List. This is a significant threat, because many ISPs use the Realtime Blackhole List to weed out spam. MAPS has been sued at least five times by direct marketing organizations objecting to being put on the list. The American Civil Liberties Union and other groups have also protested the existence of the blacklist, saying that it restricts free speech.

They have a point. Innocent Internet users can be hurt when an ISP is put on the Realtime Blackhole List. If MAPS lists an ISP, then all who use that ISP for their email account - spammers and ordinary email users alike - are blocked from sending email to large swaths of the Internet. Ordinary email users may be denied the ability to send email to family and friends subscribing to ISPs that refuse all email from networks on the Realtime Blackhole List. On the other hand, some believe this is the most effective way to get offending ISPs to change their behaviour. If the customers of an ISP complain about their email getting blocked, the ISP must choose between losing these customers and adhering to the policies set forth by MAPS.

**Proposed Solutions to the Spam Epidemic**

What is the best way to halt the spam epidemic? Here are four proposed solutions.

1. *Require an explicit opt-in of subscribers to email lists.*

A direct marketer cannot include subscribers' email addresses on a mailing list unless they have explicitly indicated that they desire to be included on the list. This proposal has two significant advantages. It would greatly increase the likelihood that people receiving commercial email will be interested in its content. It would reduce the volume of email being sent across the Internet. In July 2002 the European Union issued a directive that email lists should contain only those subscribers who have officially opted in. Member countries had until October 2003 to pass legislation enforcing this directive.

2. *Require labelling of email advertising.*

Some states passed laws requiring that all commercial emails contain the letters "ADV" in their subject line, making it easy for an individual to filter spam. These laws were preempted by the federal CAN SPAM Act, described next.

3. *Add a cost to every email that is sent.*

The primary attraction of email as an advertising medium is its low cost - a fraction of a cent per email. Advocates of this approach suggest that a system of micro­payments be established. If person A sends person B an email, person A must pay person B a few cents through an automatic system of micropayments. Marketers will no longer be able to afford to send out millions of emails, hoping that one in 100,000 persons responds.

The problem with this "solution" is that spammers often hijack other people's computers and use them to send out their massive emails. It’s the innocent own­ers of these computers, not the spammers, who would be stuck with the charges.

4. *Ban unsolicited email.*

In the late 1980s direct marketers began sending unsolicited advertisements to fax machines, tying up these machines and costing the owners time and money for supplies. In 1991 the U.S. Congress passed the Telephone Consumer Protection Act, which contained a prohibition against unsolicited faxes, called junk faxes. In March 2003 the 8th Circuit U.S. Court of Appeals upheld the ban on junk faxes. The three-judge panel ruled that "there is substantial governmental interest in protecting the public from the cost shifting and interference caused by unwanted fax advertisements".

In December 2003 President Bush signed legislation regulating commercial email sent in the United States. The Controlling the Assault of Non-Solicited Pornography and Marketing (CAN SPAM) Act of 2003 went into effect January 1, 2004.

# 

# 1-3.3 The Internet

**Is There Too Much Control Or Too Little?**

Internet access is severely limited in certain countries. The governments of Burma (Myanmar), Cuba, and North Korea make it difficult for ordinary citizens to use the Internet to communicate with the rest of the world.

In other countries Internet access is easier, but still carefully controlled. Saudi Ara­bians gained access to the Internet in 1999, after the government installed a centralized control centre outside Riyadh. Virtually all Internet traffic flows through this control centre, which blocks pornography sites, gambling sites, and many other pages deemed to be offensive to Islam or the government of Saudi Arabia. Blocked sites and pages are from such diverse categories as non-Islamic religious organizations, women's health and sexuality issues, music and movies, gay rights, Middle Eastern politics, and infor­mation about ways to circumvent Web filtering.

In contrast to Saudi Arabia, the government of the People's Republic of China does not direct all Internet traffic through a single control centre. Instead, it allows many Internet Service Providers to make their own connections outside China. However, all Internet Service Providers (including Yahoo!) have agreed to abide by a "self-discipline" agreement forbidding them from forwarding politically or morally objectionable Web pages. Besides blocking many sites containing sexually explicit material, Chinese ISPs typically block sites concerned with Chinese dissidents, sites related to Taiwan and Tibet, and many news sites, such as *BBC* News and CNN [2]. The government monitors ISPs to ensure sites that should be blocked are, in fact, unavailable to Web surfers.

Filtering within China can affect its neighbours, too. Some ISPs send packets to China with destinations beyond China (North Korea, for example). However, since Chinese routers filter packets based on the IP addresses of the originating Web server, packets simply "passing through" China can be discarded before they reach their destinations.

Meanwhile, Western nations have different standards about what is acceptable and what is not. While Germany forbids access to any neo-Nazi Web site, Web surfers in the United States can access many such sites.

Political satire and pornography are easily available through American ISPs. Amer­icans are used to political satire, but many citizens are concerned about the corrupt­ing influence of pornography, particularly with respect to minors. Since 1996 the U.S. Congress has passed three laws aimed at restricting access of children to sexually explicit materials on the Web: the Communications Decency Act, the Child Online Pro­tection Act, and the Children's Internet Protection Act. The first two laws were ruled unconstitutional by the U.S. Supreme Court; the third was upheld by the Supreme Court in June 2003.

**Challenges Posed by the Internet**

Five characteristics of the Internet make censorship more difficult.

1. *Unlike traditional one-to-many broadcast media, the internet supports many-to-many communication.*

While it is relatively easy for a government to shut down a newspaper or a radio station, it is very difficult for a government to prevent an idea from being published on the Internet, where millions of people have the ability to post Web pages.

2. *The Internet is dynamic.* .

Millions of new computers are being connected to the Internet each year.

3. *The Internet is huge*.

There is simply no way for a team of human censors to keep track of everything that is posted on the Web. While automated tools are available, they are fallible.

Hence any attempt to control access to material stored on the Internet cannot be 100 percent effective.

4. *The Internet is global.*

National governments have limited authority to restrict activities happening outside their borders.

5. *It is hard to distinguish between children and adults on the Internet.*

How can an "adult" Web site verify the age of someone attempting to enter the site?

# 1-3.4 Children and the Web

Many parents believe they ought to protect their children from exposure to porno­graphic and violent materials on the Web. A large software industry has sprung up to meet these needs

**Web Filters**

A Web filter is a piece of software that prevents certain Web pages from being displayed by your browser. While you are running your browser, the filter runs as a background process, checking every page your browser attempts to load. If the filter determines the page is objectionable, it prevents the browser from displaying it.

Filters can be installed on individual computers, or an ISP may provide filtering services for its customers. Programs designed to be installed on individual computers, such as Cyber Sentinel, eBlaster, and Spector PRO, can be set up to email parents as soon as they detect an inappropriate Web page. America Online's filtering service is called AOL Guardian. It enables parents to set the level of filtering on their children's accounts. It also allows parents to look at logs showing the pages their children have visited [2].

Typical filters use two different methods to determine if a page should be blocked. The first method is to check the URL of the page against a "blacklist" of objectionable sites. If the Web page comes from a blacklisted site, it is not displayed. The second method is to look for combinations of letters or words that may indicate a site has objectionable content.

Neither of these methods is foolproof. The Web contains millions of pages contain­ing pornography, and new sites continue to be created at a high rate; hence any blacklist of pornographic sites will be incomplete by definition. Some filters sponsored by conser­vative groups have blacklisted sites associated with liberal political causes, such as those sponsored by the National Organization of Women and gay and lesbian groups. The al­gorithms used to identify objectionable words and phrases can cause Web filters to block out legitimate Web pages.

**Child Internet Protection Act**

In March 2003 the Supreme Court weighed testimony in the case of *United States v. American Library Association.* The question: Can the government require libraries to install antipornography filters in return for receiving federal funds for Internet access?

More than 14 million people access the Internet through public library computers. About one-sixth of the libraries in the United States have already installed filtering software on at least some of their computers. The Child Internet Protection Act requires that libraries receiving federal funds to provide Internet access to its patrons must prevent children from getting access to visual depictions of obscenity and child pornography. The law allows adults who desire access to a blocked page to ask a librarian to remove the filter.

In his testimony before the Supreme Court, Solicitor General Theodore Olson argued that since libraries don't offer patrons X-rated magazines or movies, they should not be obliged to give them access to pornography over the Internet.

Paul Smith, representing the American Library Association and the American Civil Liberties Union, argued that in their attempt to screen out pornography, filters block tens of thousands of inoffensive pages. He added that requiring adults to leave the workstation, find a librarian, and ask for the filter to be turned off would be disruptive to their research and would stigmatize them.

In June 2003 the U.S. Supreme Court upheld CIPA, ruling 6-3 that antipornography filters do not violate First Amendment guarantees [7]. Chief Justice William Rehnquist wrote, "A public library does not acquire Internet terminals in order to create a public forum for Web publishers to express themselves, any more than it collects books in order to provide a public forum for the authors of books to speak. Most libraries already exclude pornography from their print collections because they deem it inappropriate for inclusion" [2].

# 1-3.5 Breaking Trust on the Internet

**Identity Theft**

Just over nine million people were victims of identity theft in 2005, and about one-eighth of these cases were computer related. How can this happen?

One can receive an email that looks authentic. The message header may be identical to the header on any popular Web site, and it would include the colour logos of Visa, MasterCard, American Express, etc. According to the message, your credit card is about to expire. So it asks you to update your personal information to avoid an interruption to your service at that web site.

The message, however, is fraudulent. If you respond with the information requested, con artists will be able to assume your electronic identity and make purchases or get cash advances using your credit card.

The attempt to deceive Internet users into disclosing personal information through the use of official-looking emails or Web sites is called phishing, and it is a growing problem. The messages appear to be from PayPal, Citibank, EarthLink, AOL, Best Buy, or other companies with which the recipient may have an account. Since many of the perpetrators of these scams are outside the United States, American law enforcement agencies have had a difficult time tracking them down and prosecuting them.

The stereotypical victim of identity theft is an elderly person who isn't computer savvy, but the facts speak otherwise. The average age of a victim of identity theft is 40. Many victims are experienced computer users who have become comfortable typing in their credit card information while online.

🏋 **Self Assessment 1-3**

1. Spam filters use the following criteria to decide which messages to block.

1. Messages with suspicious subject lines.
2. Messages coming from blacklisted ISPs.
3. A large number of messages going to the same email address.
4. A large number of messages coming from the same email address.
5. I & II only
6. II & IV only
7. I & IV only
8. I, II & III only
9. III & IV only

2. The following are some of the tactics spammers are using to confound the effects of spam blockers.

1. By using another person’s computer system as the launch pad.
2. By using images containing the message.
3. By using spam spoofing.
4. By using dumpster diving.
5. I & II only
6. II & III only
7. III & IV only
8. I, II & III only
9. I, II, III & IV only

3. What makes sending spam immoral?

1. Subject lines of messages are misleading.
2. It is unsolicited.
3. It is bulk mail.
4. It is sent because it is cheap.
5. I & II only
6. II & III only
7. III & IV only
8. I, II & III only
9. I, & III only

4. Problems created by spam include

1. A large percentage of the internet bandwidth is consumed.
2. It presents ethical problems.
3. A large amount of storage space on mail servers and individual computers is consumed.
4. It encourages phishing.
5. I & II only
6. I & III only
7. II & IV only
8. I, II & III only
9. I, III & IV only

5. Direct marketing firms build email lists through

1. Spam spoofing
2. Phishing
3. Opt-in lists
4. Dictionary attacks
5. I & II only
6. II & III only
7. III & IV only
8. I, II & III only
9. IV only

SESSION 2-3: COMPUTER AND NETWORK SECURITY

# 2-3.1 Viruses, Worms, and Trojan Horses

There are a variety of ways in which undesired programs can become active on your computer. If you are lucky, these programs will do nothing other than consume a little CPU time and some disk space. If you are not so lucky, they may destroy valuable data stored in your computer's file system. An invading program may allow outsiders to seize control of your computer. Once this happens, they may use your computer as a depository for stolen credit card information, a Web server dishing out pornographic images, or a launch pad for spam or denial-of-service attacks on a corporate server.

"Computer pathologists" classify destructive programs as viruses, worms, or Trojan horses.

Viruses

HOW VIRUSES WORK

A virus is a piece of self-replicating code embedded within another program called the host. When a user executes a host program infected with a virus, the virus code executes first. The virus finds another executable program stored in the computer's file system and replaces the program with a virus-infected program. After doing this, the virus allows the host program to execute, which is what the user expected to happen. If the virus does its work quickly enough, the user may be unaware of the presence of the virus.

Because a virus is attached to a host program, you may find viruses anywhere you can find program files: hard disks, floppy disks, CD-ROMs, email attachments, and so on. Viruses can be spread from machine to machine via diskettes or CDs. They may also be passed when a person downloads a file from the Internet. Sometimes viruses are attached to free computer games that people download and install on their computers.

Today, many viruses are spread via email. An attachment is a file accompanying an email message. Attachments may be executable programs, or they may be word processing documents or spreadsheets containing macros, which are small pieces of executable code. If the user opens an attachment containing a virus, the virus takes control of the computer, reads the user's email address book, and uses these addresses to send virus-contaminated emails to others.

Some viruses are fairly innocent; they simply replicate. These viruses occupy disk space and consume CPU time, but the harm they do is relatively minor. Other viruses are malicious and can cause significant damage to a person's file system.

WELL-KNOWN COMPUTER VIRUSES

The Brain virus was the first virus to move from one IBM PC to another. The virus was written by the owners of a Pakistani computer store called Brain Computer Services. They said their purpose was to determine the level of software piracy in Pak­istan. The virus spread internationally, but it was not malicious and caused no significant harm to the PCs it infected [8].

The Michelangelo virus dates back to 1991. If a PC user executes a program infected with the virus on March 6, the birthday of Renaissance painter and sculptor Michelangelo, the virus overwrites critical records on the boot disk. If the boot disk is the user's hard drive, the contents of the drive are lost. In 1992 the media widely reported estimates that as many as five million PCs would be affected by the virus. As it turns out, only a few thousand computers were infected. Some say the whole episode was a classic example of media hype. Others say the extensive media publicity encouraged institutions to perform checks that would not have been done otherwise. According to them, the outbreak on March 6 was not significant because institutions had already removed the virus.

The Melissa virus lurks inside a macro in a Word document attached to an email message. When a user activates the virus by opening the infected attachment, Melissa sends an email message with the attachment to the first 50 people in the user's address book. When Melissa first appeared, email containing the virus flooded the Internet, crashing many email servers worldwide. It infected about 100,000 computers in its first weekend. David L. Smith of New Jersey pled guilty to posting the virus at an alt.sex.usenet group using a stolen AOL account. In May 2001 Smith was sentenced to 20 months in federal prison plus 100 hours of community service. He was also fined $5,000 [2].

The Love Bug is another virus lurking inside an email message. Unlike Melissa, which limits itself to the first 50 people in a victim's address book, the Love Bug creates email messages for everyone in the address book. It deletes some kind of media files stored on the user’s hard disk, and it also collects passwords and emails them to several different accounts in the Philippines. The creator of the Love bug was a 23-year-old Filipino computer science student. When he created the virus, the Philippines had no laws against computer hacking, and he was not prosecuted [8].

Viruses Today

Commercial antivirus software packages allow computer users to detect and destroy viruses lurking on their computers. To be most effective, users must keep them up-to date by downloading programs corresponding to the latest viruses from the vendor's Web site.

There is evidence few people are diligent about keeping their computers virus-free. When students returned to Oberlin College in August of2003, they were required to have their computers checked for viruses. System administrators found viruses in 90 percent of the computers running the Windows operating system.

Worms

A worm is a self-contained program that spreads through a computer network by ex­ploiting security holes in the computers connected to the network. The technical term "worm" comes from *The Shockwave Rider,* a 1975 science fiction novel written by John Brunner [2].

WANK WORM

In October 1989, NASA scientists prepared for a Space Shuttle mission that would launch a probe to Jupiter. The robot probe, named Galileo, was fueled with radioactive plutonium. Antinuclear protestors created a worm that infiltrated a NASA network. Those who logged onto an infected computer were greeted with a banner with the words: **W**orms **A**gainst **N**uclear **K**illers. “Your System has been officially WANKed”

The WANK worm took a lot of system-administrator time to eradicate, but it did not delay the launch of the Space Shuttle. It is an example of cyberterrorism: a politically motivated attack against the information technology resources of a government or its people in order to inflict damage, disrupt services, or generate fear.

CODE RED

The Code Red worm, launched on July 19, 2001, exploited a bug in Microsoft's Internet Information Services (IIS) software to spread among Windows Web servers. If U.S. English was the default language on the server, the worm would change the server's local home page to the following message:

HELLO! Welcome to http://www.worm.com!

Hacked by Chinese!

Based on the day of the month, the Code Red worm either (1) attempted to propagate to other computers, (2) launched a denial-of-service attack against www.whitehouse.gov. or (3) slept. (We cover denial-of-service attacks later.) The Code Red worm spread to more than 359,000 hosts in less than 14 hours.

BLASTER

The Blaster worm appeared on August 11, 2003. It exploited a bug on Windows 2000 and Windows XP computers. Blaster infected hundreds of thousands of PCs worldwide. Besides spreading to as many computers as possible, the purpose of the Blaster worm seemed to be to launch a denial-of-service attack against windowsupdate.com, the Mi­crosoft Windows Update Web server. The apparent goal of the worm was to prevent Microsoft customers from accessing the server to download the patch needed to fix the bug. It turns out windowsupdate.com was a shortcut to the actual Web site. Microsoft thwarted the attack by deleting the shortcut.

However, the Blaster worm did have the effect of slowing down some computer systems. It disrupted the signalling of CSX freight trains and Amtrak passenger trains in the Northeast, leading to service delays.

Trojan Horses

A Trojan horse is a program with a benign capability that conceals another, sinister purpose. When the user executes a Trojan horse, the program performs the expected beneficial task. However, the program is also performing actions unknown to, and not in the best interests of, the user.

Here are a few examples of the kinds of malicious tasks performed by Trojan horse programs:

* opening an Internet connection that allows an outsider to gain access to files on the user's computer;
* logging the keystrokes of the user and storing them in a file that the attacker can peruse to learn confidential information, such as passwords;
* looking for passwords stored on the computer and emailing them to the attacker's address;
* destroying files on the user's computer;
* launching a denial-of-service attack on a Web site;
* turning the user's computer into a proxy server that can be used to launch spam or stash information gained from illegal activities (such as stolen credit card numbers).

A remote access Trojan (RAT) is a Trojan horse program that gives the attacker access to the victim's computer. Two well-known RATs are Back Orifice and SubSeven. SubSeven is notable because of its easy-to-use point-and-click user interface. SubSeven consists of a client program running on the attacker's computer, and a server program running on the victim's computer. The attacker is able to capture images from the victim's monitor, record keystrokes, read and write files, watch traffic on the victim's local area network, and even control the mouse.

In order to gain access to another person's computer, the attacker must trick that person into downloading the RAT server. The most popular way to do this is to hide it inside a file posted to a Usenet news group specializing in erotica. The attacker advertises the file as containing sexually explicit videos or photos. Those who download the file bring the RAT into their computer.

**Defensive Measures**

The ability of a computer network to withstand the attacks of viruses, worms, and Trojan horses depends to a great extent on the skill and dedication of its system administrators, as well as the cooperation of the network's users.

System administrators should set up reasonable authorization and authentication mechanisms. Authorization is the process of determining that a user has permission to perform a particular action. For example, a system administrator has authorization to reboot a computer, but a typical user does not. An ordinary user should not be able to examine the email messages of another user. Most operating systems create unique *user identifiers,* or ids, for its users. With each id is information about the user's privileges. The system administrator should set user privileges appropriately to prevent one user from violating the privacy of another.

Computer security also depends upon authentication: determining that a person is who he claims to be. There are a variety of authentication mechanisms. The most common type is knowledge-based authentication, such as a password. Another authen­tication mechanism is the use of tokens, such as an identification card or smart card. A third authentication mechanism uses biometric data, such as a fingerprint or retinal scan. It is common for highly secure computer systems to use two different authentica­tion schemes.

The most common knowledge-based authentication scheme is the password. Sys­tem administrators should install automatic password checking software that prevents users from selecting passwords that are easily guessed, such as the login name, the reverse of the login name, or a circular shift of the login name. To foil a dictionary attack ­an automated intruder attempting to guess a password by trying every word in the dictionary - a user should always have at least one non-alphabetic character in the pass­word.

A sure-fire way to prevent a network from being attacked by an external virus or worm is to detach it from the Internet. If it is important that the computers on the network be able to communicate with the Internet, installing a firewall is the next best thing. A firewall is a computer, positioned between a local network and the Internet that monitors the packets flowing in and out. One type of firewall is a packet filter, which accepts packets only from certain trusted computers on the Internet. Another use of a firewall is to limit the number of services external computers may access.

An important responsibility of the system administrator is to keep the operating system up-to-date with the latest patches. When the provider of an operating system announces a security patch, the announcement also informs malicious persons that a vulnerability exists. Sometimes a new worm is launched well after the patch has been made available. Up-to-date systems are not vulnerable to attacks by these worms.

A system administrator can install filters on mail servers that screen out much unwanted mail, including spam and virus-laden email. Still some contaminated email messages are likely to get through to individual users. Virus filters associated with email readers can check incoming messages for viruses. When such a message is found, it is deleted or put in a quarantine area.

# 2-3.2 Hackers

Telephone and computer systems are powerful technologies, prompting some curious people to invest a lot of time and energy into learning more about how they work. A few of these experts use the knowledge they have gained to enter systems without authorization. Once inside these systems, their actions vary widely, from simply "nosing around" to copying sensitive information to rerouting phone calls. In this section we examine the activities of and hackers.

ORIGINAL DEFINITION OF "HACKER"

In its original meaning, a hacker is an explorer, a risk-taker, someone who is trying to make a system do something it has never done before. Hackers in this sense of the word abounded at MIT's Tech Model Railroad Club in the 1950s and 1960s. The Club constructed and continuously improved an enormous HO-scale model train layout. Members of the Signals and Power Subcommittee built an elaborate electronic switch­ing system to control the movement of the trains. Wearing chino pants, short-sleeved shirts, and pocket protectors, the most dedicated members would drink vast quantities of Coca-Cola and stay up all night to improve the system. To them, a "hack" was a newly constructed piece of equipment that not only served a useful purpose, but also demon­strated its creator's technical virtuosity. Calling someone a hacker was a sign of respect; hackers wore the label with pride. In 1959, after taking a newly created course in computer programming, some of the hackers shifted their attention from model trains to electronic computers.

Computer security expert Dorothy Denning has observed that the will of the hacker is to make an improvement - a hacker is not malicious. A hacker is not out to destroy data or equipment. A hacker does not commit fraud for personal profit.

MALICIOUS HACKERS

In the modern use of the word, "hacking" has come to include computer break-ins accompanied by malicious behaviour, such as destroying databases or stealing confidential personal information.

DUMPSTER DIVING AND SOCIAL ENGINEERING

Typically, you need a login name and password to access a computer system. Sometimes a hacker can guess a valid login name/password combination, particularly when system administrators allow users to choose short passwords or passwords that appear in a dictionary. Two other effective techniques for obtaining login names and passwords are dumpster diving and social engineering.

“Dumpster diving” means looking through garbage for interesting bits of information. Companies typically do not put a fence around their dumpsters. In midnight rum­maging sessions hackers have found user manuals, phone numbers, login names, and passwords.

Social engineering, a term coined by hacker Kevin Mitnick, refers to the manipulation of a person inside the organization to gain access to confidential information. Social engineering is easier in large organizations where people do not know each other very well. For example, a hacker may identify a system administrator and call that person, pretending to be the supervisor of his supervisor and demanding to know why he can't access a particular machine. In this situation, a cowed system administrator, eager to please his boss's boss, may be talked into revealing or resetting a password.

Penalties for Hacking

Under U.S. law, the maximum penalties for hacking are severe. The Computer Fraud and Abuse Act criminalizes a wide variety of hacker-related activities, including:

* transmitting code (such as a virus or worm) that causes damage to a computer system;
* accessing without authorization any computer connected to the Internet, *even if no files are examined, changed, or copied;*
* transmitting classified government information;
* trafficking in computer passwords;
* computer fraud;
* computer extortion.

The maximum penalty imposed for violating the Computer Fraud and Abuse Act is 20 years in prison and a $250,000 fine.

Another federal statute related to computer hacking is the Electronic Communica­tions Privacy Act. This law makes it illegal to intercept telephone conversations, email, or any other data transmissions. It also makes it a crime to access stored email messages without authorization.

The use of the Internet to commit fraud or transmit funds can be prosecuted under the Wire Fraud Act and/or the National Stolen Property Act. Adopting the identity of another person to carry out an illegal activity is a violation of the Identity Theft and Assumption Deterrence Act.

# 2-3.3 Denial-of-Service Attacks

A Denial-of-Service (DoS) attack is an intentional action designed to prevent legitimate users from making use of a computer service. A DoS attack may involve unauthorized access to one or more computer systems, but the goal of a DoS attack is not to steal information. Instead, the aim of a DoS attack is to disrupt a computer server's ability to respond to its clients. Interfering with the normal use of computer services can result in significant harm. A company selling products and services over the Internet may lose business. A military organization may find its communications disrupted. A nonprofit organization may be unable to get its message out to the public.

A DoS attack is an example of an "asymmetric" attack, in which a single person can harm a huge organization, such as a multinational corporation or even a government. Since terrorist organizations specialize in asymmetric attacks, some fear that DoS attacks will become an important part of the terrorist arsenal.

During the week of February 7-11, 2000, a 15-year-old initiated DoS attacks that disabled many Web sites, including Amazon.com, eBay, Yahoo, CNN.com, and Dell. The teenager, who went by the nickname "Mafiaboy," was sentenced to eight months in a juvenile detention centre and a year of probation.

In October 2002 a DoS attack was launched against the Internet's 13 root servers, which act as the Internet's ultimate authority with respect to matching domain names to IP addresses.

Recently, many DoS attacks have focused on blacklist services, used by ISPs to shield their customers from spam. "We're usually under attack from 5,000 to 10,000 servers at once;” says Steve Linford, CEO of Spamhaus.

Let’s take a look at the different kinds of DoS attacks and some of the defensive measures that organizations can take to guard themselves against such attacks. Attackers do not want to give themselves away by initiating attacks from their own systems. Instead, they identify other computers they can use to launch their attacks. For this reason, all system administrators, not just those at targeted organizations, play a role in preventing DoS attacks.

**Attacks that Consume Scarce Resources**

The most common DoS attack is against a target system's network connection. A low-tech but effective way to do this is to cut the physical connection between the target computer and its network. Hence it is important that organizations provide their servers with adequate physical security.

Another form of network attack consumes all the bandwidth on the target's net­work by generating a large number of messages directed to that network. The smurf attack is an example of this form of DoS attack. The attacker first identifies routers that support broadcasting of messages to all of the computers on their local area networks. The attacker sends "ping" messages to these routers, which multiply them. A computer receiving a "ping" message is supposed to echo it. In this case, the attacker has spoofed the IP address, making it look as if the ping came from the target computer. All of the computers receiving the ping message send an echo to the target computer. In a successful attack, the flood of incoming messages saturates the target server's network.

In a third kind of DoS attack, the attacker attempts to fill all of the available space on the target computer's disk. Here are three ways to fill a target computer's disk:

1. In email bombing, the attacker sends the target a flood of email messages. The target computer stores these email messages on its disk. By sending very long messages, the attacker can quickly fill the target's disk drive. Email bombing is usually combined with email spoofing (changing the email address of the sender) to disguise the identity of the attacker from the target.

2. The attacker creates a worm that intentionally generates a very long stream of errors. Since the target computer logs errors in a data file, eventually the disk fills up.

3. The attacker breaks in to the target computer and copies over files from another site.

Most computers have a limit on the number of processes that may be active at one time. An attacker can disable the target's computer by penetrating it with a worm program that quickly replicates. (This is how Morris's Internet worm crashed many of the computers it infected.) Even if the target computer does not crash, the presence of many active processes can significantly degrade the performance of the computer's CPU.

Another form of DoS attack crashes the target computer by sending it unexpected data, such as an oversized IP packet.

Defensive Measures

System administrators can take a variety of defensive measures to reduce the threat of DoS attacks throughout the Internet.

Ensuring the physical security of a server is an important defensive measure. Beyond the server itself, physical security encompasses the network access point, the wiring closet, and the air conditioning and power systems.

System administrators should benchmark the performance of their computer systems in order to establish baselines. Once the baselines are known, it is easier to detect aberrations that may indicate a breach of security.

Disk quota systems are another good security measure. If single users have limits on the amount of disk space they may use, then it is tougher for an intruder to create files that eat up all the disk space. Disabling unused network services is another prudent policy. Reducing available services reduces the options given potential attackers.

Another security measure is turning off the amplifier network capability of routers, taking a weapon out of the hands of those who wish to launch a smurf attack.

Companies have begun to create pattern-recognition software to detect DoS attacks. The software is used to discard requests for service that are coming from "clients" that have proven to be unreliable.

### 🏋 Self Assessment 2-3

1. I am a piece of computer code. I attach myself to a host program and execute when my host executes. You may find me on CD-ROMs, email attachments, etc. I am fairly innocent, simply replicating. Who am I?

1. A Virus
2. A Trojan horse
3. A Worm
4. A Cookie
5. A Spyware

2. This was the first known virus to move from one IBM PC to another. It was written by the owners of a Pakistani computer store to determine the level of software piracy. Which virus is this?

1. The Melissa virus
2. The Love bug
3. The Brain Virus
4. The Michelangelo virus
5. The Red code

3. I am a program that lurked inside email messages and created email messages for everyone in the victims address book. I also collected passwords and emailed them to several accounts in the Philippines. What is my name?

1. The Melissa virus
2. The Love bug
3. The Brain Virus
4. The Michelangelo virus
5. The Red code

4. The following is/are common authentication mechanisms used by system administrators.

I. Use of biometric data

II. Use of passwords

III. Use of identification cards

1. I & II only
2. I & III only
3. II & III only
4. I, II & III
5. II only

5. Which of these may be used to launch a denial of service attack on a web site?

1. Viruses
2. RATs
3. Mice
4. Worms
5. Cookies

 ***Learning Track Activities***

|  |  |
| --- | --- |
| j0299125 | **Unit Assignments 3**  1. What is spam?  2. Explain how MAPS attempts to reduce the amount of spam people receive.  3. What is the difference between a computer virus and a computer worm?  5. 4. Why is it dangerous for an email program to open attachments automatically, without waiting for the user to select them?  5. What is a Denial-of-Service attack? |
|  |  |

Unit 4

INFORMATION RIGHTS: PRIVACY AND FREEDOM IN AN INFORMATION SOCIETY

**Introduction**

What is **privacy**? It is the claim of individuals to be left alone, free from surveillance by or interference from other individuals or organizations, including the state. Privacy is the right of people not to reveal information about themselves, i.e. the right to keep personal information, such as medical histories, personal e-mail messages, student records and financial information from getting into wrong hands.

But what do we see? Millions of employees are subject to electronic and other forms of high-tech surveillance. Computers and the Internet have accelerated the rate at which organizations can collect, exchange, combine, and distribute information about individuals. All these capabilities make it a challenge to preserve your privacy. Information Technology and Information Systems threaten individual claims to privacy by making the invasion of privacy cheap, profitable and effective, thus putting constant pressure on this right to privacy.

In 1890, US Supreme Court Justice Louis Brandeis stated that the “right to be left alone” is one of the most comprehensive of rights and the most valued by civilized man [9]. With Information Systems, privacy deals with the collection and use or misuse of data. Data is constantly being collected and stored on each of us. This data is often distributed over easily accessed networks and without our knowledge or consent.

In this unit we focus on the privacy issues related to the introduction of information technology. We begin by taking a philosophical look at privacy. What is privacy? Do we have a natural right to privacy distinct from other rights, such as the right to property and the right to liberty?

We then take a look at some of the ways that we leave an “electronic trail” of information behind us as we go about our daily lives. Both private organizations and governments construct databases documenting our activities.

Identity theft is an increasingly common crime. We describe a variety of ways in which thieves steal credit card numbers and other personal and financial information.

One powerful tool for preserving one’s privacy in the information age is through the use of encryption. We explain this technology next.

A variety of laws have been passed in the United States to regulate the collection and distribution of information gathered by private and public entities. We shall briefly discuss some of these laws.

Finally we describe some suggested solutions to some of the privacy problems that the introduction of IT brings.

|  |  |
| --- | --- |
| j0293844 | **Learning Objectives**  After reading this unit you should be able to:   1. Outline a few of the numerous threats to privacy 2. Understand the philosophers view on privacy 3. Recognize ways in which we intentionally or unintentionally disclose information about ourselves 4. Recognize a variety of ways identity theft is orchestrated 5. Explain the technique of data encryption |

Unit content

**Session 1-4: Philosophical Look at Privacy and the Electronic Trail**

1-4.1 Threats to Privacy

1-4.2 Perspective on Privacy

1-4.3 Disclosing Information

1-4.4 Public Information

1-4.5 Public record

**Session 2-4: Other Privacy concerns raised by New Technology & Laws on Privacy**

2-4.1 Identity Theft

2-4.2 Encryption

2-4.3 Rules and Laws on Privacy

2-4.4 Some Suggested Solutions

SESSION 1-4: Philosophical Look at Privacy and the Electronic Trail

# 1-4.1 Threats to Privacy

Do you for instance think that your *medical records* are inviolable? Actually private medical information is bought and sold freely by various companies in many advanced countries like the United States since there is no federal law prohibiting it. In 1993 Maryland created a database containing medical records of its residents. The purpose of the database was to help the state find ways to contain health care costs. A member of Maryland's public health commission, who happened to be a banker, had access to the database. He used this information to call in the loans of his customers who had cancer [2].

How about for example *student records in colleges or universities*? Actually attorneys, auditors, therapists and some others can view them now. In addition, colleges are now implementing systems of transferring transcripts, disciplinary reports, and other student reports by electronic means. A privacy advocate, Gorden Cook, has warned that “Brick by innocent brick the edifice of lifelong electronic students dossiers is being constructed without any recognition by the general public of what is been done” [10].

Someone in campus security at Georgetown University accidentally sent out to the entire campus community an email crime report containing the names of three students. To protect these students, system administrators shut down the email system at George town University for several hours and deleted the offending email from the mailboxes of the recipients. This incident illustrates the power of modern communication net works to broadcast personal information at high speed. It's also a reminder that system administrators have the ability to read our email messages [2].

What about adequate controls on *financial information* collected about you? Pray you are not a victim of ***identity theft***, one of the fastest growing forms of fraud. A relatively new crime, identity theft is the stealing of identifying information about you – from loan documents, credit card offers, bank statements, utility bills and the like – then using it to establish new credit accounts.

On the morning of July 18, 1989, actress Rebecca Schaeffer opened the door to her apartment and was shot to death by obsessed fan Robert Bardo. Bardo got Schaeffer's home address from a private investigator who purchased her driver's license information from the California Department of Motor Vehicles. In response to this murder, the U.S. Congress passed the Driver's Privacy Protection Act in 1994. The law prohibits states from revealing certain personal information provided by drivers in order to obtain licenses. It also requires states to provide this information to the federal government [2].

Is an employee guaranteed of *privacy at the work place*? Currently, the right of workers who want their privacy and the interest of companies that demand to know more about their employees are in conflict. Recently companies have been monitoring their workers via computer technology. These computer-monitoring systems tie directly into workstations; specialized computer programs can track every keystroke made by the user. This type of system can determine what workers are doing while at the keyboard. The system also knows when the worker is not using the keyboard or computer system. These systems can estimate what a person is doing and how many breaks he or she is taking. Needles to say, many workers consider this close supervision very dehumanizing.

When using your *e-mail at work* do you think that your boss cannot snoop on your e-mail? The law allows employers to “intercept” employee communication if one of the parties involved agrees to the interception. The party involved in this case is the employer. Indeed, employer snooping seems to be widespread. Thus a good rule of thumb, suggest one writer, is to “think of an e-mail message not as a sealed letter but as a postcard – and, even more a postcard that might well be read and copied in every post office it passes through, then kept on file for years after”.

Furthermore, e-mail messages which have been erased from hard disks may be retrieved and used in lawsuits because the law of discovery demands that companies produce all relevant business documents.

All these private information gathering about people mostly without their permission is made possible and easy because of advances in database technology and the use of electronic networks such as the Internet which were mentioned earlier. These are considered again next.

Databases

Large organizations around the world are constantly compiling information about most of us. Worldwide the number of online databases – 70% of which are in the United States – has skyrocketed from 400 in 1980 to 10s of thousands in 1996 [10].

The means by which related records are pulled together in databases is the use of a key field to do the linking. In the US, the Social Security Number is the most frequently used key field though it was not intended to be used as a “universal identifier” but rather for the collection of taxes for the federal administered retirement system and for disbursing its payments to individuals. Unfortunately one’s Social Security number can be obtained from a number of sources.

Professional data gatherers or “information resellers” collect personal data and sell it to fund-raisers, direct marketers, and others. In the US, even some motor-vehicle departments sell the car-registration data they store. From this database, companies have been able to collect names, addresses, and other information about the majority of American households. Some privacy experts estimate that the average person is on 100 mailing lists and in 50 databases at one time.

Electronic Networks

When one surfs the net, he /she assumes nobody knows where they go or what they do. But that is wrong. The danger of the Internet now is the illusion of anonymity that’s completely false.

Say you visit a cigarette company’s web site and give it your name and e-mail address in order to get discount coupons for cigarettes. The web site deposits on your computer – a so-called **cookie**, a special file that keeps track of your activities and visits to other sites. The cookie can connect your name or e-mail address to any future visit to that web site. You do not have to be notified that this information is being gathered. Worst still, there are practically no restrictions on how the information may be disseminated or otherwise used. Thus, for example, your health or insurance company could eventually get hold of the information and decide to raise the premium of people it believes are smokers.

On line services such as AOL, CompuServe, MSN, and Prodigy can and do sell information about you to be used for direct marketing purposes. Most (but not all) of the services allow you to specify that you don’t want information about you disclosed in this way, but you have to take the initiative.

It is very important for a Website to have a policy explaining how personal information is used, and the policy statement must make people feel comfortable and be extremely clear about what information is collected and what will and will not be done with it. However, many web sites do not prominently display their privacy policy or implement practices completely consistent with that policy.

Most people using the Internet rely on privacy by obscurity. That is, they believe that the sheer volume of data that flows over the net each day will keep browsing anonymous. But tracing your travel on the net is probably easier than you think.

With today’s computers therefore, the right to privacy is an especially challenging problem. When someone is born, take certain high school exams, starts working, enrols in a college or university course, applies for a driver’s license, purchase a car, gets married, gets insured, registers at a library, applies for a credit card or opens a bank account, purchase a house or take a mortgage, or indeed buys a host of other products, data is collected and stored somewhere in a computer database. The difficult question to answer is “Who owns this information and knowledge? If a private or public organization spends time and resources to obtain data on you, does the organization own the data and can it use the data in any way it desires? In the US, government legislation answers these questions to some extent for federal agencies, but the question remains unanswered for private organizations.

# 1-4.2 Perspective on Privacy

Philosophers struggle to define privacy. Discussions about privacy revolve around the notion of *access,* where access means either physical proximity to a person or knowledge about that person. There is a tug of war between the desires, rights, and responsibilities of a person who wants to restrict access to himself, and the desires, rights, and responsibilities of outsiders to gain access.

Edmund Byrne takes the point of view of the individual seeking to restrict access when he defines privacy as a **"zone of inaccessibility"** that surrounds a person.

You have privacy to the extent that you can control who has access into your zone of inaccessibility. For example, you exercise your privacy when you lock the door behind you when using the toilet. You also exercise your privacy when you choose not to tell the clerk at the video store your Social Security number. However, privacy is not the same thing as being alone. Two people can have a private relationship. It might be a physical relationship, in which each person lets the other person become physically close while excluding others. It might be an intellectual relationship, in which they exchange letters containing private thoughts.

When we look at privacy from the point of view of outsiders seeking access, the discussion revolves around where to draw the line between what is private and what is public (known to all). As Edward Bloustein has pointed out, stepping over this line and violating someone's privacy is an affront to that person's dignity [2]. You violate someone's privacy when you treat him or her as a means to an end. Put another way, some things ought not to be known.

On the other hand, society can be harmed if individuals have too much privacy. Some people take advantage of privacy to plan and carry out illegal or immoral activities. Most wrongdoing takes place under the cover of privacy. For example most terrorism or coup plots are orchestrated under the cover of privacy. If members of a private club share information with each other that is not available to the general public and the club facilitates business deals among its members, it may give them an unfair advantage over others in the community who are just as capable of fulfilling contracts. In this way privacy can encourage social and economic inequities, and the public at large may benefit if the group had less privacy (or its membership were more diverse). Here is an example of a public/private conflict, suppose a journalist learns that a wealthy candidate for high public office has half a dozen lovers. Does the public interest outweigh the politician's desire for privacy in this case?

Some benefits of privacy are that; socialization and individuation are both necessary steps for a person to reach maturity. Privacy is necessary for a person to blossom as an indi­vidual. Privacy is recognition of each person's true freedom. Privacy lets us be ourselves and be able to "blow off steam". Privacy can foster intellectual activities. It also allows us to shut out the rest of the world so that we can focus our thoughts without interruption. Privacy is needed for spiritual growth, the opportunity to become intimate with the Absolute Being. Privacy is the only way in which people can develop relationships involving respect, love, friendship, and trust.

James Rachels writes that "there is a close connection between our ability to control who has access to us and to information about us, and our ability to create and maintain different sorts of social relationships with different people". Charles Sykes echoes Rachels when he says that each person has a "ladder" of privacy. At the top of the ladder is the person we share the most information with. For many people this person is their spouse. As we work our way down the ladder, we encounter people we would share progressively less information with. Here is an example of what some one's ladder of privacy might look like [2]:

Spouse, priest/minister/rabbi, brothers and sisters, parents, children, friends, in-laws, coworkers, neighbours, marketers, employers, government, news media, ex-spouses, potential rivals/enemies.

In summary, privacy is a social arrangement that allows individuals to have some level of control over who is able to gain access to their physical selves and their personal information.

Most of us agree that every person has certain natural rights, such as the right to life, the right to liberty, and the right to own property. Many people also talk about our right to privacy. Is this a natural right as well? The next few paragraphs that follow might help you answer this question.

Privacy and Trust

While many people complain about threats to privacy, it is clear upon reflection that we have more privacy than our ancestors did. Charles Sykes writes: "Over the past two centuries, the rise of the modern has been the rise of the individual" [11]. The consequence of all this privacy is that we live among strangers. Many people know little more about their neighbours than their names (if that). Yet when we live in a society with others, we must be able to trust them to some extent. How do we know that the taxi driver will get us where we want to go without hurting us or overcharging us? How do parents know that their children's teachers are not child molesters? How does the bank know that if it loans someone money, it will be repaid?

In order to trust others, we must rely on their reputations. This was easier in the past, when people didn't move around so much and everyone knew everyone else's history. Today, society must get information out of people to establish reputations. As Steven Nock puts it, ''A society of strangers is one of immense personal privacy. Surveillance is the cost of that privacy" [2].

# 1-4.3 Disclosing Information

As we go about our lives, we leave behind an electronic trail of our activities, thanks to computerized databases. Databases record the purchases we make with credit cards, the groceries we buy at a discount with our loyalty cards, the videos we rent by showing our driver's licenses, the calls we make with our telephones, and much more. The companies collecting this information use it to bill us. They also can use this information to serve us better. For example, Amazon.com uses information about book purchases to build profiles of its customers. With a customer profile, Amazon.com can recommend other books the customer may be interested in buying [2].

It's important to distinguish between public information and public records. A public record contains information about an incident or action reported to a govern­ment agency for the purpose of informing the public. Examples of public records are birth certificates, marriage licenses, motor vehicle records, criminal records, and deeds to property.

Public information is information you have provided to an organization that has the right to share it with other organizations. A good example of public information is a listing in a telephone directory. Most of us allow our name, address, and phone number to appear in telephone directories. By doing this, it is easier for our friends and acquaintances to call us or stop by our home. We judge this benefit to be worth the cost to us in the form of less privacy.

Personal information is information that is not public information or part of a public record. You may rightly consider your religion to be personal information. It remains personal information as long as you never disclose it to an organization that has the right to share it. However, if you do disclose your religious affiliation to such an organization, it becomes public information.

Personal information becomes public information or a public record through a voluntary, involuntary, or statutory disclosure

Often people voluntarily make personal information public. Product registration forms and contest entries often ask consumers to reveal a great deal of personal information.

Sometimes you must disclose information in order to get something you want. If you want to fly on an airplane, you must allow others to search your luggage. You may even be subjected to a body search. You cannot refuse these searches if you want to travel by air. If you want to get a loan from a bank, you must provide the bank with your full name and Social Security number (so it can do a credit check), as well as detailed information about current income, your assets, and your liabilities. If you want to get married, you must fill out a marriage license and submit yourself to whatever tests are required by the local jurisdiction.

At other times, personal information becomes a public record without your con­sent. Police agencies and courts maintain records of arrests and convictions. Divorce records are public, and they can contain a significant amount of personal information.

Finally, information is sometimes gathered without our knowledge. There are more than a half million closed-circuit television cameras installed in public places in England. A resident of London may be captured on tape many times every day. A principal reason for installing these cameras is to reduce crime. However, detractors of this system point to abuses. Some allege that prosecutors have destroyed video footage that may have cleared a suspect. Others say that camera operators have acted like high-tech peeping Toms, using the cameras to watch people having sex.

# 1-4.4 Public Information

In this section we survey just a few of the many ways that personal information can become public information.

Rewards or Loyalty Programs

Today, many shoppers take advantage of rewards programs sponsored by grocery stores. Card-carrying members of the store's "club" save money on many of their purchases, either through coupons or instant discounts at the cash register. The most significant difference between the Green Stamps program and a contemporary shopper's club is that today's rewards programs are run by computers that record every purchase. Companies can use information about the buying habits of particular customers to provide them with individualized service.

Body Scanners

In some stores in the United Kingdom, you can enter a booth, strip to your under­garments, and be scanned by a computer, which produces a three-dimensional model of your body. The computer uses this information to recommend which pairs of jeans ought to fit you the best. You can then sit in front of a computer screen and preview what various pairs of jeans will look like on you. When you have narrowed down your search to a few particular brands and sizes, you can actually try on the jeans.

Digital Video Recorders

TiVo, Inc. manufactures a digital video recorder (DVR), which is similar to a VCR except that it records TV programs on a hard disk instead of videotape. TiVo also provides a service that allows its subscribers to more easily record programs they are interested in watching later. For example, with a single command a subscriber can instruct the TiVo to record every episode of a TV series. What many consumers may not know is that TiVo sells detailed information about the viewing habits of its customers. Because the system monitors the activities of the user second by second, its data are more valuable than that provided by other services. For example, TiVo's records show that 54 percent of its customers skip commercials [2].

Automobile "Black Boxes"

You probably know about airplane flight data recorders, also called "black boxes;' which provide information useful in postcrash investigations. Did you know that modern automobiles also come equipped with a "black box"? A microprocessor attached to the car's airbag records information about the speed of the car, the amount of pressure being put on the brake pedal, and whether the seat belts are connected. After a collision, investigators can retrieve the microprocessor from the automobile and view data collected in the five seconds before the accident.

Enhanced 911 Service

The U.S. Federal Communications Commission has passed an enhanced 911 mandate that requires cell phone providers to be able to track the locations of active cell phone users to within 100 meter. The safety benefit of enhanced 911 service is obvious. Emergency response teams can reach people in distress even if they are unable to speak or do not know exactly where they are.

The ability to identify the location of active cell phone users has other benefits. For example, it makes it easier for cell phone companies to identify where signal strength is weak and coverage needs to be improved. In the past, this information had to be gained by sending people into the field to check signal strength.

The downside to enhanced 911 services is loss of privacy. Because it is possible to track the location of active cell phone users, what happens if information is sold or shared? Suppose you call your employer and tell him you are too sick to come into work on a Good Friday. Your boss is suspicious; since this is the third Good Friday in the past three years you've called in sick. Your employer pays your cell phone provider and discovers that you made your call from the Kwahu ridge.

RFIDs

Imagine getting up in the morning, walking into the bathroom, and seeing a message on the medicine cabinet's computer screen warning you that your bottle of aspirin is close to its expiration date. Later that day, you are shopping for a new pair of pants. As you try them on, a screen in the dressing room displays other pieces of clothing that would complement your selection.

These scenarios are possible today thanks to a new technology called RFID, short for radio frequency identification. An RFID is a tiny wireless transmitter. Manufacturers are replacing bar codes with RFIDs, because they give more information about the product and are easier to scan. An RFID can contain specific information about the particular item to which it is attached (or embedded), and a scanner can read an RFID from six feet away. When barcodes are replaced by RFIDs, check-outs are quicker and companies track their inventory more accurately.

However, because RFIDs are not turned off when an item is purchased, the new technology has raised privacy concerns. Imagine a workplace full of RFID scanners. A scanner in your cubicle enables a monitoring system to associate you with the tags in your clothes. Another scanner picks up your presence at the water cooler. The next thing you know, your boss has called you in for a heart-to-heart talk about how many breaks you're taking. Some privacy advocates say consumers should have a way to remove or disable RFIDs in the products they purchase

The U.S. government plans to replace traditional passports with electronic passports equipped with RFID tags. The RFID tag would duplicate the passport's identifying information and include a digital photograph. By combining the RFID tag's informa­tion with new facial recognition technology, the government hopes to improve security at border crossings. Critics of this plan say that RFID tags can be read by anyone within 25 feet who has a powerful enough chip reader. They fear that these tags could make travelers more vulnerable to identity theft. Others wonder if terrorists with power­ful RFID tag readers might begin "scanning" foreign cafes, searching for locations with a high concentration of Americans. Some experts, however, claim that these fears are exaggerated and that RFID tags are difficult to read at a distance.

Implanted Chips

In Taiwan every domesticated dog must contain a microchip implant identifying its owner and residence. The microchip, about the size of a grain of rice, is implanted into the dog's ear using a syringe.

Digital Angel Corporation has created a personal safety and location system that includes a clip-on monitor about the size of a pager, a temperature sensing watch, and a global positioning system. The system is designed to monitor an elderly person's location and environment, and to send an alert when necessary. For example, the system generates an alert if the subscriber falls down and doesn't get up. It also generates an alert if the subscriber wanders outside of a predetermined neighbourhood.

Some people believe that parents should implant microchips in their children. They say that the life of a child is more important than any concerns about privacy.

Cookies

A cookie is a file placed on your computer's hard drive by a Web server. The file contains information about your visits to a Web site. Cookies can contain login names and passwords, product preferences, and the contents of virtual "shopping carts." Web sites use cookies to provide you with personalized services, such as custom Web pages. Instead of asking you to type in the same information multiple times, a Web site can retrieve that information from a cookie. Most Web sites do not ask for permission before creating a cookie on your hard drive. You can configure your Web browser to alert you when a cookie is being placed on your computer, oryou can set your Web browser to refuse to accept any cookies. However, some Web sites cannot be accessed by browsers that block cookies.

Spyware

Spyware is a program that communicates overyour Internet connection without your knowledge or consent. Spyware programs can monitor Web surfing, log keystrokes, take snapshots ofyour computer screen, summon pop-up advertisements, and send reports back to a host computer.

Free software downloaded fromthe Internet often contains spyware. A 2003 survey of 120 U.S. consumers with broadband Internet connections found that 91 percent ofthem had spyware on their computers.

Some ISPs are responding to the outbreak ofspyware by releasing tools to help their customers protect their privacy. America Online plans to start including spyware-detecting programs with its software distribution.

# 1-4.5 Public record

The federal government maintains thousands of databases containing billions of records about the activities of U.S. citizens. In this section we consider the public-record-keeping activities of the Census Bureau, the Internal Revenue Service, and the FBI, paying par­ticular attention to ways in which information collected for one purpose often has been used for another.

Census Records

In order to ensure each state has fair representation in the House of Representatives, the United States Constitution requires the government to perform a census every 10 years.

The first census of 1790 had six questions. It asked for the name of the head of the household and the number of persons in each of the following categories: free white males at least 16 years old; free white males under 16 years old; free white females; all other free persons (by sex and colour); and slaves.

As time passed, the number of questions asked during the census increased. The 1820 census determined the number of people engaged in agriculture, commerce, and manufacturing. The 1840 census had questions regarding school attendance, illiteracy, and occupations. In 1850 census takers began asking questions about taxes, schools, crime, wages, and property values. The 1940 census is notable because for the first time statistical sampling was put to extensive use. A random sample of the population, about five percent of those surveyed, received a longer form with more questions. The use of sampling enabled the Census Bureau to produce detailed demographic profiles without substantially increasing the amount of data it needed to process.

Internal Revenue Service Records

Your income tax form may reveal a tremendous amount of personal information about your income, your assets, the organizations to which you give charitable contribu­tions, your medical expenses, and much more. Every year the IRS investigates hundreds of employees for misusing their access to these records. In one notable case, a member of the Ku Klux Klan examined records of fellow Klan members, hoping to identify a sus­pected undercover agent in his group. The IRS has also misplaced hundreds of tapes and diskettes containing income tax data.

FBI National Crime Information Center 2000

The FBI National Crime Information Centre 2000 (NCIC) is a collection of databases supporting the activities of federal, state, and local law-enforcement agencies in the United States, the United States Virgin Islands, Puerto Rico, and Canada. Its pre­decessor, the National Crime Information Centre, was established by the FBI in January 1967 under the direction of J. Edgar Hoover [2].

When it was first activated, the NCIC consisted of about 95,000 records in five databases: stolen automobiles, stolen license plates, stolen or missing guns, other stolen items, and missing persons. Today, NCIC databases contain more than 39 million records. The databases have been expanded to include such categories as wanted persons, criminal histories; people incarcerated in federal prisons, convicted sex offenders, unidentified persons, people believed to be a threat to the President, foreign fugitives, violent gang members, and suspected terrorists. More than 80,000 law enforcement agencies have access to these data files. The NCIC processes more than two million requests for information each day, with an average response time of less than one second.

* The FBI points to the following successes of the NCIC: investigating the assassination of Dr. Martin Luther King, Jr., the NCIC provide the FBI with the information it needed to link a fingerprint on the murder weapon to James Earl Ray.
* In 1992 the NCIC led to the apprehension of 81,750 "wanted" persons, 113,293 arrests, the location of 39,268 missing juveniles and 8,549 missing adults, and the retrieval of 110,681 stolen cars.
* About an hour after the April 19, 1995, bombing of the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma state trooper Charles Hanger pulled over a Mercury Marquis with no license plates. Seeing a gun in the back seat of the car, Hanger arrested the driver-Timothy McVeigh-on the charge of transporting a loaded firearm in a motor vehicle. He took McVeigh to the county jail, and the arrest was duly entered into the NCIC database. Two days later, when federal agents ran McVeigh's name through the NCIC, they saw Hanger's arrest record. FBI agents reached the jail just before McVeigh was released. McVeigh was subsequently convicted of the bombing.

Critics of the National Crime Information Centre point out ways in which the existence of the NCIC has led to privacy violations of innocent people:

* Erroneous records can lead law enforcement agencies to arrest innocent persons. . Innocent people have been arrested because their name is the same as someone listed in the arrest warrants database.
* The FBI has used the NCIC to keep records about people not suspected of any crime, such as opponents of the Vietnam War.
* Corrupt employees o flaw-enforcement organizations with access to the NCIC have sold information to private investigators and altered or deleted records.
* People with access to the NCIC have illegally used it to search for criminal records on acquaintances or to screen potential employees, such as baby-sitters [2].

🏋 **Self Assessment 1-4**

1. There is a \_\_\_\_\_\_\_\_\_\_\_ right to intellectual property.

1. Natural
2. Weak
3. Strong
4. Negative
5. Artificial

2. It is possible for more than one person to owe an intellectual property. True or false?

1. True
2. False

3. Which of these has contributed significantly to increasing our privacy in recent times?

1. Religion
2. Single-family home
3. Television
4. ICT
5. Education
6. I & II only
7. I & III only
8. II & III only
9. II, III & IV only
10. III, IV & V only

4. Which of these are considered as public information?

1. Telephone directory listing
2. Marriage licenses
3. Motor vehicle records
4. I & II only
5. I & III only
6. II & III only
7. I only
8. I, II & III only

5. One can voluntarily make personal information private through

1. product registration
2. participating in loyalty programs
3. contest entries.
4. I & II only
5. I & III only
6. II & III only
7. III only
8. I, II & III only

SESSION 2-4: OTHER PRIVACY CONCERNS & LAWS ON PRIVACY

# 2-4.1 Identity Theft

Dorothy Denning defines identity theft as "the misuse of another person's identity, such as name, Social Security number, driver's license, credit card numbers, and bank account numbers. The objective is to take actions permitted to the owner of the identity, such as withdraw funds, transfer money, charge purchases, get access to information, or issue documents and letters under the victim's identity".

The leading form of identity theft in United States is credit card fraud. Identity thieves either take out a new credit card in someone else's name or commandeer an existing account. By changing the billing address of existing accounts, a thief can run up large debts before the victim becomes aware of the problem. These activities can blemish the target's credit history. As a result, victims of identity theft may have appli­cations for credit cards, mortgage loans, and even employment denied. If the impostor shows false credentials to the police, the victim may even be saddled with a false criminal record or outstanding arrest warrants. Financial institutions contribute to the problem of identity theft by making it easy for people to open up new accounts. Since information brokers on the Web are selling driver's license numbers, Social Security numbers, and credit card information, it's easy for an identity thief to gather a great deal of information about another person. Assuming another person's identity is made simpler by banks allowing people to open accounts online.

According to Privacy Rights Clearinghouse, more than 27 million Americans were victims of identity theft between 2000 and 2004. The frequency of identity theft is increasing; there were nearly 10 million identity theft victims in 2004. The average loss in 2004 was about $5,000 per victim.

Fortunately, United States law says that a consumer's liability for losses due to credit card fraud is limited to $50 if reported promptly. Many financial institutions do not even collect this amount . However, victims of identity theft typically spend hundreds of hours cleaning up their financial records.

Most cases of identity theft are not the result of someone using computers to break into a database containing information about a target. Instead, identity thieves are much more likely to use low-tech methods to gain access to the personal information they need. Two popular sources of information are mailboxes and lost or stolen wallets. One in six cases of identity theft are traced to family members, friends, or co workers.

Some identity thieves 'engage in dumpster diving-looking for personal infor­mation in garbage cans or recycling bins. Old bills, bank statements, and credit card statements contain a wealth of personal information, including names, addresses, and account numbers. Another simple way to get information is through shoulder surfing looking over the shoulders of people filling out forms.

More recently, thieves have begun using skimmers (also called wedges) to steal credit card data. A skimmer is a small, battery-powered credit card reader. Identity theft rings use skimmers to collect hundreds of credit card numbers, and then use these numbers to manufacture counterfeit credit cards. Credit card numbers are collected by waiters or store clerks, who match each legal swipe through a cash register with an illegal swipe through a skimmer. In one case, someone attached a skimmer to an ATM along with a sign requesting customers to use the "card cleaner" before putting their card in the ATM.

Some thieves send out spam messages designed to look like they originated from PayPal, eBay, or another well-known Internet-active business. Through these messages they hope to con unsuspecting recipients into revealing their credit card numbers or other personal information. Gathering financial information via spam is called phishing (pronounced "fishing").

Large institutions that store personal data are tempting targets for information thieves. Between 2003 and 2005 criminals used stolen passwords to access LexisNexis databases 59 times, retrieving the Social Security numbers and other financial informa­tion of more than 300,000 people. ChoicePoint disclosed that it accidentally gave con artists access to about 150,000 personal financial dossiers, and Bank of America lost computer tapes containing information about more than a million federal employees.

A hacker broke into a T-Mobile database and downloaded the photographs and personal information of at least 400 customers.

The Identity Theft and Assumption Act of 1998 makes identity theft a federal crime. In 2004 Congress passed the Identity Theft Penalty Enhancement Act, which length­ened prison sentences for identity thieves. A variety of law enforcement agencies investigate alleged violations of this law: the U.S. Secret Service, the FBI, the U.S. Postal Inspection Service, and the Office of the Inspector General of the Social Security Ad­ministration. Unfortunately, the probability that a particular case of identity theft will result in an arrest is about 1 in 700.

The rapid increase in the number of identity theft victims is prompting new ques­tions about how people identify themselves. In the United States, the Social Security number is a common form of identification, even though that was not how it was origi­nally conceived.

# 2-4.2 Encryption

Encryption is the process of transforming a message in order to conceal its meaning. In an age in which information is easily captured and rebroadcast, encryption is a valuable tool for maintaining privacy. Even if someone should get a copy of an encrypted message, it is worthless unless the person can decode it.

Symmetric Encryption

In a traditional symmetric encryption scheme, a single key is needed to encrypt and decrypt a message. Suppose Smith wants to send a message to Jones. Smith and Jones are the only two people to know the key. Smith uses the key to encrypt the message into cipher. Jones uses the key to decrypt the cipher back into the message. Since no one else has the key, even if the cipher should fall into the wrong hands, it cannot be read. The weakness of symmetric encryption schemes is that it does not solve the problem of how Smith gets the key to Jones. If a hostile outsider should get a copy of the key as it is transmitted, the security of the system is broken

Public-Key Cryptography

The key transmission problem was solved by Whitfield Diffie and Martin Hellman, who published an alternative scheme, called public-key cryptography, in 1976. Public-key encryption is an example of asymmetric encryption because it uses two keys instead of one. Each person has a public key and a private key. A message encrypted with the public key can only be decrypted with the private key. That means everybody who wants to *receive* encrypted messages announces their public keys. If Smith wants to send an encrypted message to Jones, he uses *Jones's* public key. After Jones receives the cipher, he uses his private key to decrypt it. Public-key cryptography eliminates the Achilles heel of symmetric encryption schemes, because no longer is there a need for people to exchange keys. Figure 5.6 illustrates how the RSA public-key encryption algorithm works.

There is a mathematical relationship among the public and private keys, and it is theoretically possible to determine the private key from the public key. The time needed to determine the private key increases with the length of the key. We say encryption is weak if a computer can guess the private key from the public key in a reasonably small amount of time. In contrast, encryption is strong if the amount of time needed by a computer to guess the private key is so long that decryption is essentially impossible. For example, it may be possible for a computer to decipher a strongly encrypted message in 2,000 years, but by that time it probably will make no difference. Strong encryption is possible by choosing a long enough public key.

As we have seen, various federal agencies perform surveillance operations to fight crime and maintain the national security. The work of these agencies is simplified if they have the ability to read domestic and foreign messages. If messages are weakly encrypted, their work is still possible because they have high-speed computers that can decipher the messages. However, if messages are strongly encrypted, their work is made much more difficult. The traditional policy of the United States has been to regulate the use of cryptography within the United States and to forbid the exportation of strong encryption technology.

# 2-4.3 Rules And Laws on Privacy

In the past few decades, significant laws have been passed in the United States and European countries regarding an individual’s right to privacy. Others relate to business privacy rights and the fair use of data and information.

Most American and European privacy law is based on a regime called **Fair Information Practice (FIP)**. FIP is a set of principles governing the collection and use of information about individuals. In the United States, the major piece of legislation on privacy is the **Privacy Act of 1974 (PA74)**. PA74 however does not apply to certain federal agencies such as the CIA and law enforcement agencies.

Privacy Act of 1974

In the early 1970s*,* William Richardson, the Secretary of the U.S. Department of Health, Education, and Welfare, convened a group to recommend policies for the development of government databases that would protect the privacy of American citizens. The Secre­tary's Advisory Committee of Automated Personal Data Systems, Records, Computers, and the Rights of Citizens produced a report for Congress, which included the following "bill of rights" for the Information Age:

CODE OF FAIR INFORMATION PRACTICES

1. There must be no personal data record-keeping systems whose very existence is secret.

2. There must be a way for a person to find out what information about the person is in a record and how it is used.

3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.

4. There must be a way for a person to correct or amend a record of identifiable information about the person.

5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

Interestingly, the Richardson report had a greater impact in Europe than in the United States. Nearly every nation in Europe passed laws based on the Code of Fair Information Practices.

The Privacy Act of 1974 represents Congress's codification of these principles. While the Privacy Act does allow individuals in some cases to get access to federal files containing information about them, in other respects it has fallen short of the desires of privacy advocates. In particular, they say the Privacy Act has not been effective in reduc­ing the flow of personal information into governmental databases, preventing agencies from sharing information with each other, or preventing unauthorized access to the data. They claim agencies have been unresponsive to outside attempts to bring them into alignment with the provisions of the Privacy Act. The Privacy Act has the following principal limitations:

1. *The Privacy Act applies only to government databases.*

Far more information is held in private databases, which are excluded. This is an enormous loophole, because government agencies can purchase information from private organizations that have the data they want.

2. *The Privacy Act only covers records indexed by a personal identifier.*

Records about individuals that are not indexed by name or another identifying number are excluded. For example, a former IRS agent tried to gain access to a file containing derogatory information about himself, but the judge ruled he did not have a right to see the file, since it was indexed under the name of the IRS investigator, not the IRS agent.

3*. No* *one in the federal government is in charge of enforcing the provisions of the Privacy*

*Act.*

Federal agencies have taken it upon themselves to determine which databases they can exempt. The IRS has exempted its database containing the names of taxpayers it is investigating. The Department of Justice has announced that the FBI does not have to ensure the reliability of the data in its NCIC databases.

4. *The Privacy Act allows one agency to share records with another agency as long as they are for a "routine use."*

Each agency is able to decide for itself what "routine use" means. The Department of Justice has encouraged agencies to define "routine use" as broadly as possible.

The FIP principles are based on the notion of a “mutuality of interest” among the record holder and the individual. The individual has an interest in engaging in a transaction. And the record keeper – usually a business or government agency – requires information about the individual to support the transaction. Once the information is gathered, the individual maintains an interest in the record, and the record may not be used to support other activities without the individual’s consent.

Other US Federal Privacy Laws

There are a number of federal legislation relating to privacy in the US, some of which are mentioned here.

* *Fair Credit Reporting Act of 1970 (FCRA*). -This act regulates operations of credit –reporting bureaus, including how they collect, store, and use credit information.
* *Right to Financial Privacy Act of 1978. -*This act restricts government access to certain records held by financial institutions.
* *Freedom of Information Act of 1970 -*This act guarantees access for individuals to personal data collected about them and about government activities in federal institutions.
* *Computer Matching and Privacy Act of 1988* - This act regulates cross-referencing between federal agencies’ computer files (e.g. to verify eligibility for federal programs).
* *Computer Abuse Amendments Act of 1994 -* This act prohibits the transmission of harmful computer programs and code, including viruses.
* *Gramm-Leach-Bliley Act* of 1999 - This act requires all financial institutions to protect and secure customer’s nonpublic data from unauthorized access or use.
* *USA Patriot Act of 2001 -* The 2001 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA Patriot) was passed in response to the September 11 terrorism acts. Proponents argue that it gives necessary new powers to both domestic law enforcement and international intelligence agencies. Critics argue that the law removes many of the checks and balances that previously allowed the courts to ensure law enforcement agencies did not abuse their powers. For example, under this act, Internet service providers and telephone companies must turn over customer information, including number called, without a court order if the FBI claims that the records are relevant to a terrorism investigation. Also, the company is forbidden to disclose that the FBI is conducting an investigation.

In the United States, privacy law is enforced by individuals who must sue agencies or companies in court in order to recover damages. European countries and Canada define privacy in a similar manner to the United States, but they have chosen to enforce their privacy laws by creating Privacy Commissions or Data Protection Agencies to pursue complaints brought by citizens.

# 2-4.4 Some Suggested Solutions

As a way of combating these problems and preventing governments from dictating Internet privacy standards, a group called the **Online Privacy Alliance** is developing a voluntary code of conduct. It is backed by companies such as Apple Computers, AT&T, Boeing, Dell, DoubleClick, eBay, IBM, Microsoft, Time Warner, Verizion Communications, and Yahoo! The alliance’s guidelines call on companies to notify users when they are collecting data at Web sites to gain consent for all uses of that data, to provide for the enforcement of privacy policies, and to have a clear process in place for receiving and addressing user complaints.

Another possible solution to some consumer privacy concerns is the screening technology called the **Platform for Privacy Preferences (P3P)** being proposed to shield users from sites that don’t provide the level of privacy protection they desire. Instead of forcing users to find and read through the private policy for each site they visit, P3P software in a computer’s browser will download the privacy policy from each site, and notify the user if the policy does not match his or her preferences. The World Wide Web Consortium, an international industry group whose members include Apple, Commerce One, Ericsson, and Microsoft, is supporting the development of P3P.

🏋 **Self Assessment 2-4**

1. Identity thieves may use \_\_\_\_\_\_\_\_\_\_\_\_\_ in obtaining personal information about their targeted victim.

1. Skimmers
2. Phishing
3. Dumpster diving
4. Shoulder surfing
5. I & II only
6. I & III only
7. II & III only
8. I, II, & III only
9. I, II, III & IV

2. It is impossible to determine one’s private key for decryption of a cipher message if the public key is known. True or false?

1. True
2. False

3. The U.S. Privacy Act of 1974 has the following principal limitations

1. The Privacy Act allows one agency to share records with another agency as long as they are for a "routine use."
2. The Privacy Act does not apply to government databases
3. The Privacy Act only covers records indexed by a personal identifier.
4. I & II only
5. I & III only
6. II & III only
7. I only
8. I, II & III

4. This act requires all financial institutions to protect and secure customer’s nonpublic data from unauthorized access or use.

1. Fair Credit Reporting Act of 1970
2. Freedom of Information Act of 1970
3. Gramm-Leach-Bliley Act of 1999
4. Right to Financial Privacy Act of 1978
5. USA Patriot Act of 2001

5. European countries enforce their privacy laws by

I. individuals who must sue agencies or companies in court to recover damages

II. creating data protection agencies

III. creating privacy commissions

1. I & II only
2. I & III only
3. II & III only
4. I, II & III
5. III only

 *Learning Track Activities*

|  |  |
| --- | --- |
| j0299125 | **Unit Assignments 4**   1. Briefly give three (3) reasons why the right to privacy is an especially challenging problem in this Information Age. 2. State any four (4) of the five Fair Information Practice principles. 3. What are the main concerns of privacy campaigners regarding the USA Patriots Act of 2001? 4. Briefly describe three (3) methods that Identity Thieves use to gain access to personal information they need. |

Unit 5

INTELLECTUAL PROPERTY

Introduction

The ability to store music in digital form has combined with the high communication speed of the Internet to create a legal crisis. A poll by Ipsos-Reid says that more than 60 million Americans have used the Internet to download music [2].

About 95 percent of "Microsoft" products purchased in China are actually counterfeits made by Chinese entrepreneurs [2]. Microsoft does not receive revenues from these sales; it calls the entrepreneurs "software pirates."

As a society we benefit from access to high-quality music, movies, computer programs, and other products of the human intellect. The value of these intellectual properties is much higher than the value of the media on which they are distributed. Creating the first copy is very expensive. Duplicates cost almost nothing. There is a strong incentive for people to make unauthorized copies. When this happens, producers of intellectual property do not receive all of the payments the law says they are entitled to. The legal system has responded by giving more rights to the creators of intellectual property. Are these changes in the best interests of our society, or are our politicians catering to special interest groups?

In this unit we discuss how IT is affecting our notion of intellectual property. We consider what makes intellectual property different from tangible property and how governments have created a variety of mechanisms to guarantee intellectual property rights. We examine what has been considered as “fair” use of intellectual property created by others, and how new copy-protection technologies are eroding the notion of fair use. We also explore the evolution of intellectual property protection for computer software and the rise of the open-source movement, which advocates the distribution of source code to programs.

|  |  |
| --- | --- |
| j0293844 | Learning Objectives  After reading this unit you should be able to:   1. Differentiate between intellectual property and physical property 2. Recognize the benefits and limitations of intellectual property protection 3. Be acquainted with legal tools available for intellectual property protection. 4. Recognize circumstances under which copyrighted work may be legally reproduced under fair use. 5. Define and understand the beneficial consequences of Open-source software. |

Unit content

**Session 1-5: Intellectual Property Rights**

1-5.1 Intellectual Property

1-5.2 Benefits And Limits to Intellectual Property Protection

1-5.3 Legal Protection for Intellectual Property

1-5.4 Fair Use

**Session 2-5: Protection for Propriety Software & Open Source Software**

2-5.1 Software Copyrights

2-5.2 Software Patents

2-5.3 Consequences of Proprietary Software

2-5.4 Definition of Open-Source

2-5.5 Beneficial Consequences of Open-Source Software

SESSION 1-5: Intellectual Property Rights

# 1-5.1 What Is Intellectual Property?

Intellectual property is any unique product of the human intellect that has commercial value. Examples of intellectual property are books, songs, movies, paintings, inventions, chemical formulas, and computer programs.

It is important to distinguish between intellectual property and its physical manifestation in some medium. If a poet composes a new poem, the poem itself is the intellectual property, not the piece of paper on which the poem is printed.

In modern Western democracies there is a widely accepted notion that people have the right to own property. Does this right extend to intellectual property as well? To answer this question, we need to examine the philosophical justification for a natural right to property.

Property Rights

The English philosopher John Locke (1632-1704) developed an influential theory of property rights. In *The Second Treatise of Government,* Locke makes the following case for a natural right to property. First, people have a right to property in their own person. Nobody has a right to the person of anybody else. Second, people have a right to their own labour. The work that people perform should be to their own benefit. Third, people have a right to those things that they have removed from Nature through their own labour [2].

For example, suppose you are living in a village in the middle of the woods, which are held in common. One day you walk into the woods, chop down a tree, saw it into logs, and split the logs into firewood. Before you cut down the tree, everyone had a common right to it. By the time you have finished splitting the logs, you have mixed your labour with the wood, and at that point, it has become your property. Whether you burn the wood in your stove, sell it to someone else, pile it up for the winter, or give it away, the choice of what to do with the wood is yours.

Locke uses the same reasoning to explain how a person can gain the right to a piece of land. Taking a parcel out of the state of Nature by clearing the trees, tilling the soil, and planting and harvesting crops gives people who performed these labours the right to call the land their property.

To Locke, this definition of property makes sense as long as two conditions hold. First, no person claims more property than he or she can use. In the case of harvesting a natural resource, it is wrong for someone to take so much that some of it is wasted. For example, people should not appropriate more land than they can tend. Second, when people remove something from the common state in order to make it their own property, there is still plenty left over for others to claim through their labour. If the woods are full of trees, I can chop a tree into firewood without denying you or anyone else the opportunity to do the same thing.

Locke's description of a natural right to property is most useful at explaining how virtually unlimited resources are initially appropriated. It is not as useful in situations where there are few or no resources left for appropriation.

Extending the Argument to Intellectual Property.

Is there a natural right to intellectual property?

We can try to demonstrate such a right exists by extending Locke's theory of property rights to intellectual property. We should however bear in mind that Locke was talking about the ownership of physical objects and we are talking about the ownership of ideas. We'll compare creating a piece of intellectual property to making a belt buckle. In order to make a belt buckle, a person must mine ore, smelt it down, and cast it. To write a play, a playwright "mines" words from the English language, "smelts" them into stirring prose, and "casts" them into a finished play [2].

It is *possible* for two people to come up with the same piece of intellectual property, such as a play, even though they laboured independently i.e. neither of the two people seeing the other’s work: even though this is highly unlikely.

If we apply Locke's theory of property to this situation, clearly both writers have the right to own the play.They mixed their labour with the raw resources of the English language and produced a play. Here we are talking about the sequence of words comprising the play not the piece of paper upon which the words of the play are written. The paper is simply a way of conveying the play or intellectual property.

Each one of them should have certain rights from his or her ownership of the play. They should have the right to decide who will perform the play. They should have the right to require others who are performing the play to pay them a fee, etc.

If two people go to the same iron mine, dig ore, smelt it, and cast it into belt buckles, there are two belt buckles, one for each person. Even if the belt buckles look identical, they are distinct, and we can give each person ownership of one of them. This is not the case with intellectual property*.* Even though they both worked independently, there is only one play*.* Whether we give one person complete ownership or divide the ownership among the two men, both cannot get full ownership of the play, which is what they ought to have if the analogy were perfect. Therefore, the uniqueness of intellectual properties is the first way in which they differ from physical objects. Intellectual property is different from physical property in the sense that it is possible for more than one person to have full ownership of the same thing.

Again, consider that one of the writers did not labour to come up with his own play, but made a photocopy of the play (or perhaps read the play) and left the original copy without the owner knowing.

Can we say this is stealing? The first writer who is the actual owner still has his physical copy of the play, but he has lost exclusive control over who will read, perform, or hear the play. If you want to call this stealing, then stealing in the sense of intellectual property is quite different from stealing a physical object. When you steal someone's car, they can't drive it any more. When you steal someone's joke, both of you can tell it.

Certainly any creator of a piece of intellectual property has the right to keep his ideas a secret. The owner could have locked it in a trunk to prevent others from seeing it. The second writer would not have the right to break into the first writer’s trunk to get access to the play. Hence we can argue that there is a natural right to keep an idea confidential. Unfortunately, this is a weak right, because the owner cannot perform the play while he is keeping it confidential. He must give up the confidentiality in order to put his creation to good use.

We began this section with the question - Is there a natural right to intellectual property? We have found no right other than the weak right to keep an idea confidential. In our quest for stronger rights, we have uncovered two important differences between tangible property and intellectual property. First, every intellectual property is one-of-a-kind. Second, copying a piece of intellectual property is different from stealing a physical object.

# 1-5.2 Benefits And Limits to Intellectual Property Protection

Benefits of Intellectual Property Protection

New ideas in the form of inventions and artistic works can improve the quality of life for the members of a society. Some people are philanthropic and will gladly share their creative energies. For example, Benjamin Franklin (1706-1790) invented many useful items, including an improved wood stove, the lightning rod, the odometer, and bifocals. He did not patent any of them. Franklin said, "As we enjoy great advantages from the invention of others, we should be glad of an opportunity to serve others by any invention of ours; and this we should do freely and generously" [2]. However, most people find the allure of wealth to be a strong inducement for labouring long hours in the hope of creating something useful. **Hence even if there are no natural rights to intellectual property, a society may choose to grant intellectual property rights to people because of the beneficial consequences**.

The authors of the Constitution of the United States recognized the benefits society reaps by encouraging creativity. Article I, Section 8, of the U.S. Constitution gives Congress the power to "promote the Progress of Science and useful Arts by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."

If a person has the right to control the distribution and use of a piece of intellectual property, there are many opportunities for that person to make money. For example, suppose you build a better mousetrap and the government gives you ownership of this design. You may choose to manufacture the mousetrap yourself. Anyone who wants the better mousetrap must buy it from you, because no other mousetrap manufacturer has the right to copy your design. Alternatively, you may choose to license your design to other manufacturers, who will pay you for the right to build mousetraps according to your design [2].

Limits to Intellectual Property Protection

Of course, society benefits the most when inventions are in the public domain and anyone can take advantage of them. Going back to the mousetrap example, we would like everyone in society who needs a mousetrap to get the best possible trap. If someone invents a superior mousetrap, the maximum benefit would result if all mousetrap manufacturers were able to use the better design. On the other hand, if the inventor of the superior mousetrap did not have any expectation of profiting from her new design, she may not have bothered to invent it. Hence there is a tension between the need to reward the creators of intellectual property by giving them exclusive rights to their ideas and the need to disseminate these ideas as widely as possible.

The way the Congress has traditionally addressed this tension is through a compromise. It has granted authors and inventors exclusive rights to their writings and discoveries, but only for a finite period of time. At the end of that time period, the intellectual property enters the public domain. While creators have control over the distribution of their properties, use of the properties is more expensive, and the creators are rewarded. After properties enter the public domain, using them becomes less expensive, and everyone has the opportunity to produce derivative works from them.

Consider a community orchestra that wishes to perform a piece of classical music. It may purchase a piece of music from the public domain for far less money than it cost simply to rent the same piece of music while it was still protected by copyright.

# 1-5.3 Legal Protection for Intellectual Property

While the U.S. Constitution gives Congress the right to grant authors and inventors exclusive rights to their creations, it does not elaborate on how these rights will be protected. Today, there are four different ways in which individuals and organizations protect their intellectual property: trade secrets, patents, copyrights, and trademarks/service marks.

Trade Secrets

A trade secret is a confidential piece of intellectual property that provides a company with a competitive advantage. Examples of trade secrets include formulas, processes, proprietary designs, strategic plans, customer lists, and other collections of information. The right of a company to protect its trade secrets is widely recognized by governments around the world. In order to maintain its rights to a trade secret, a company must take active measures to keep it from being discovered. For example, companies typically require employees with access to a trade secret to execute a confidentiality agreements.

A famous trade secret is the formula for Coca-Cola syrup. The formula, known inside the company as "Merchandise 7X," is locked in a bank vault in Atlanta, Georgia. Only a few people within the company know the entire formula, and they have signed nondisclosure agreements. The task of making the syrup is divided among different groups of employees. Each group makes only one part of the final mixture, so that nobody in these groups learns the complete recipe.

An advantage of trade secrets is that they do not expire. A company never has to disclose a trade secret. Coca-Cola has kept its formula secret for more than 100 years.

The value of trade secrets is in their confidentiality. Hence trade secrets are not an appropriate way to protect many forms of intellectual property. For example, it would make no sense for a company to make a movie a trade secret, because a company can only profit from a movie by allowing it to be viewed, which would make it no longer confidential. On the other hand, it would be appropriate for a company to make the *idea* for a movie a trade secret.

While it is illegal to steal a trade secret, there are other ways in which the confidentiality may be broken. "Reverse engineering" is one way in which a competing firm can legally gain access to information contained in a trade secret. If another company can purchase a can of Coca-Cola and figure out the formula, it is free to manufacture a soft drink that looks and tastes just like Coke.

Another way in which a competing firm can gain access to information contained in another company's trade secret is by hiring its employees. While a firm can require its employees to sign confidentiality agreements, it cannot erase the memories of an employee who starts working for a competing firm. Hence some "leakage" of confidential information may be inevitable when employees move from one company to another.

**Trademarks and Service Marks**

A trademark is a word, symbol, picture, sound, colour, or smell used by a business to identify goods. A service mark is a mark identifying a service.

By granting a trademark or service mark, a government gives a company the right to use it and the right to prevent other companies from using it. Through the use of a trademark, a company can establish a "brand name." Society benefits from branding because branding allows consumers to have more confidence in the quality of the products they purchase.

When a company is the first to market a distinctive product, it runs the risk that its brand name will become a common noun used to describe any similar product. When this happens, the company may lose its right to exclusive use of the brand name. Some trademarks that have become generic are "yo yo," "aspirin," "escalator," "thermos;' and "brassiere:' Companies strive to ensure their marks are used as adjectives rather than nouns.

Patents

A patent is a way governments provide an inventor with an exclusive right to a piece of intellectual property. A patent is quite different from a trade secret because a patent is a public document that provides a detailed description of the invention. The owner of the patent can prevent others from making, using, or selling the invention for the lifetime of the patent, which is currently 20 years. After the patent expires, anyone has the right to make use of its ideas.

*POLAROID V. KODAK*

Dr. Edwin Land invented "instant" photography. The company he founded, Polaroid Corporation, had 10 patents protecting the invention of film that developed in 60 seconds. Polaroid did not license these patents to other firms, and for many years it was the only company to sell cameras and film allowing photographs to be developed in a minute.

When Kodak introduced its first instant camera in 1976, Polaroid sued Kodak. In 1985 a court ruled that Kodak had infringed on seven of Polaroid's original ten patents; six years later Kodak paid Polaroid a $925 million settlement [12].

Copyrights

A copyright is how the U.S. government provides authors with certain rights to original works that they have written.Copyright is a statutory grant that protects creators of intellectual property against copying by others for any purpose for a period of 95 years. Copyright protection is extended to books, periodicals, lectures, drama, musicals compositions, maps, drawings, artwork of any kind, and motion pictures. It also protects software. Copyright protection is automatic; you do not have to register your idea with the government (as you do with a patent) in order to receive protection. The intent behind copyright laws has been to encourage creativity and authorship by ensuring that creative people receive the financial and other benefits of their work.

The owner of a copyright has five principal rights:

1. The right to reproduce the copyrighted work

2. The right to distribute copies of the work to the public

3. The right to display copies of the work in public

4. The right to perform the work in public

5. The right to produce new works derived from the copyrighted work

Copyright owners have the right to authorize others to exercise these five rights with respect to their works. The owner of a copyright to a play may sell a license to a high school drama club that wishes to perform it. After a radio station broadcasts a song, it must pay the songwriter(s) and the composer(s) through a performance rights organization.

Copyright owners have the right to prevent others from infringing on their rights to control the reproduction, distribution, display, performance, and production of works derived from their copyrighted work.

Several important industries in the United States, including the movie industry, music industry, software industry, and book publishing, rely upon copyright law for protection. "Copyright industries" account for over 5 percent of the United States gross domestic product, with over $500 billion in sales. About 5 million U.S. citizens work in these industries, which are growing at a much faster rate than the rest of the U.S. economy. With foreign sales and exports of $89 billion, copyright industries were the leading export sector in the United States in 2001 [2].

In this section we examine court cases and legislation that have helped define the limits of copyright in the United States.

In the 1980s Kinko's Graphics Corporation engaged in what it called the "Professor Publishing" business. It distributed brochures to university professors asking them to provide lists of readings they planned to use in their courses. Kinko's used these lists to produce packets of reading materials for students taking these classes. The packets typically contained chapters from books. In 1991 the U.S. District Court for the Southern District of New York ruled that when Kinko's produced these packets it infringed upon the copyrights held by the publishers. The judge ordered Kinko's to pay statutory damages of $510,000 to the plaintiffs, a group of eight book publishers. Kinko's subsequently got out of the Professor Publishing business [2].

DAVEY JONES LOCKER

Richard Kenadek ran a computer bulletin board system (BBS) called Davey Jones Locker. Subscribers paid $99 a year for access to the BBS, which contained copies of more than 200 commercial programs. In 1994 Kenadek was indicted for infringing on the copyrights of the owners of the software. He pleaded guilty and was sentenced to six months' home confinement and two years' probation [2].

NO ELECTRONIC THEFT ACT

Another incident in 1994 led to further legislation protecting copyrights. David LaMaccia, an MIT student, posted copyrighted software on a public bulletin board he created on a university computer. According to prosecutors, bulletin board users downloaded more than a million dollars' worth of software in less than two months. However, the prosecutors were forced to drop charges against LaMaccia because he had made the programs available for free. Since he had not profited from his actions, he had not violated copyright law. To close this legal loophole, Congress passed the No Electronic Theft Act of 1997, which made it a criminal offence *simply to reproduce or distribute* more than $1,000 worth of copyrighted material in a six-month period [2].

COPYRIGHT CREEP

Currently, works created and published before January I, 1978, are protected for 95 years. Works created on or after January 1, 1978, are protected for the author's lifetime plus 70 years after the author's death. If the work is a work made for hire, the length of protection is 95 years from the date of publication or 120 years from the date of creation, whichever is less.

According to Siva Vaidhyanathan, "in the early republic and the first century of American legal history, copyright was a Madisonian compromise, a necessary evil, a limited, artificial monopoly, not to be granted or expanded lightly". Over time, however, Congress has gradually increased both the term of copyright protection and the kind of intellectual properties that are protected by copyright. One reason has been the desire to have international copyright agreements. In order to complete these agreements, Congress has had to reconcile American copyright law with European law, which in general has had much stronger protections for the producers of intellectual property. Another reason for "copyright creep" has been the introduction of new technologies such as photography, audio recording, and video recording [2].

# 1-5.4 Fair Use

The right given to a copyright owner to reproduce a work is a limited right. Under some circumstances, called fair use, it is legal to reproduce a copyrighted work without the permission of the copyright holder. Examples of fair use include citing short excerpts from copyrighted works for the purpose of teaching, scholarship, research, criticism, commentary, and news reporting.

The United States Copyright Act does not precisely list the kinds of copying that are fair use. Instead, what is considered to be fair use has been determined by the judicial system. The courts have relied upon Section 107 of the Copyright Act, which lists four factors that need to be considered:

1. *What is the purpose and character of the use?*

An educational use is more likely to be permissible than a commercial use.

2. *What is the nature of the work being copied?*

Use of nonfiction is more likely to be permissible than use of fiction. Published works are preferred over unpublished works.

3. *How much of the copyrighted work is being used?*

Brief excerpts are more likely to be permissible than entire chapters.

4. *How will this use affect the market for the copyrighted work?*

Use of out-of-print material is more likely to be permissible than use of a readily available work. A spontaneously chosen selection is better than an assigned reading in the course syllabus.

Let's consider two scenarios in which copyrighted works are duplicated and determine if they made fair use of the material.

FAIR USE EXAMPLE 1

A professor puts a few journal articles on reserve in the library and makes them assigned reading for the class. Some students in the class complain that they cannot get access to the articles because other students always seem to have them checked out. The professor scans them and posts them on his Web site. The professor gives the students in the class the password they need to access the articles.

The first factor to consider is the purpose of the use. In this case the purpose is strictly educational. Hence this factor weighs in favour of fair use.

The second factor is the nature of the work being copied. The journal articles are non-fiction. Again this weighs in favour of fair use.

The third factor is the amount of material being copied. The fact that the professor is copying entire articles rather than brief excerpts weighs against a ruling of fair use.

The fourth factor is the effect the copying will have on the market for journal sales. If the journal issues containing these articles are no longer for sale, then the professor's actions cannot affect the market. The professor took care to prevent people outside the class from accessing the articles. Overall, this factor appears to weigh in favour of fair use.

Three of the four factors weigh in favour of fair use. The professor's actions probably constitute fair use of the copyrighted material.

FAIR USE EXAMPLE 2

An art professor takes slide photographs of a number of paintings reproduced in a book about Renaissance artists. She uses the slides in her class lectures.

The first factor to consider is the purpose of the copying. The professor's purpose is strictly educational. Hence the first factor weighs in favour of fair use.

The second factor is the type of material being copied. The material is art. Hence this factor weighs against a ruling of fair use.

The third factor is the amount of material copied. In this case the professor is displaying copies of the paintings in their entirety. Fair use almost never allows a work to be copied in its entirety. Note that even if the original painting is in the public domain, the photograph of the painting appearing in the art book is probably copyrighted.

The final factor is the effect the copying will have on the market. The determination of this factor would depend on how many images the professor took from anyone book and whether the publisher is in the business of selling slides of individual images appearing in its book.

Overall, this professor's actions are less likely to be considered fair use than the actions of the professor in the first scenario.

***Sony vr. Universal City Studios***

In 1975 Sony introduced its Betamax system, the first consumer VCR. People used these systems to record television shows for viewing later, a practice called time shifting. Some customers recorded entire movies onto videotape.

A year later, Universal City Studios and Walt Disney Productions sued Sony, saying it was responsible for copyright infringements performed by those who had purchased VCRs. The movie studios sought monetary damages from Sony and an injunction against the manufacturing and marketing of VCRs. The legal battle went all the way to the U.S. Supreme Court. The Supreme Court evaluated the case in light of the four fair use factors.

The first factor is the intended purpose of the copying. Since the purpose is private, not commercial, time shifting should be seen as fair use with respect to the first factor.

The second factor is the nature of the copied work. Consumers who are time shifting are copying creative work. This would tend to weigh against a ruling of fair use.

The third factor is the amount of material copied. Since a consumer copies the entire work, this weighs against a ruling of fair use.

The final factor is the affect time shifting will have on the market for the work. The Court determined that the studios were unable to demonstrate that time shifting had eroded the commercial value of their copyrights. The movie studios receive large fees from television stations in return for allowing their movies to be broadcast. Television stations can pay these large fees to the studios because they receive income from advertisers. Advertising rates depend upon the size of the audience; the larger the audience, the more a television station can charge an advertiser to broadcast a commercial. Time shifting allows people who would not ordinarily be able to watch a show to view it later. Hence it can be argued that VCRs actually increase the size of the audience, and since audience size determines the fees studios receive to have their movies broadcast on television, it is not at all clear whether the copying of these programs harms the studios.

The Supreme Court ruled, in a 5-4 decision, that time shifting television programs is a fair use of the copyrighted materials. It said that the private, noncommercial use of copyrighted materials ought to be presumed fair use unless it could be shown that the copyright holder would be likely to suffer economic harm from the consumer's actions. Importantly, the Court also noted that the Sony Betamax VCR could be used to copy both copyrighted and noncopyrighted material, and that Sony should not be held accountable if some of the people who buy a VCR choose to use it to infringe on copyrights [2].

RIAA v. Diamond Multimedia Systems Inc*.*

Diamond Multimedia Systems introduced the Rio portable music player in 1998. About the size of an audio cassette, the Rio stored an hour of digitized music. The Recording Industry Association of America (RIAA) asked for an injunction preventing Diamond Multimedia Systems from manufacturing and distributing the Rio. The RIAA alleged that the Rio did not meet the requirements for the Audio Home Recording Act of 1992, because it did not employ a Serial Copyright Management System to prevent unauthorized copying of copyrighted material.

The U.S. Court of Appeals, Ninth Circuit, upheld the ruling of a lower court that the Rio was not a digital audio recording device as defined by the Audio Home Recording Act. It denied the injunction on these technical grounds. In addition, the Court affirmed that space shifting, or copying a recording in order to make it portable, is fair use and entirely consistent with copyright law.

Digital Technology and Fair Use

In the not-so-distant past, music publishers distributed content on vinyl records, and some purchasers made copies onto cassette tapes. The copying process introduced hiss and distortions that significantly degraded the quality of the music. Trying to make a copy from a copy resulted in a nearly worthless tape. Music publishers focused on suing major violators of copyright law (those producing thousands of tapes) and ignored people who made a few copies of albums for their friends.

Three technological innovations disrupted the status quo. The first advance was the compact disc (CD). Initially, the introduction of CDs was a huge boon for the music publishing industry. The per-unit production costs of CDs was lower than vinyl albums or tapes, but their sound quality was higher, meaning companies could charge more for them. As a result, their profits swelled.

However, because a CD encodes music digitally - as a stream of ones and zeros - it can be copied perfectly. Now that CD burners are standard equipment on personal computers, millions of people have the ability to clone music CDs. Since each copy is perfect, a copy of a copy is as good as the original. Blank CDs cost only a few cents. CDs sold in stores often cost nearly 20 dollars. Respecting copyright law has become an expensive proposition.

Digital reproduction means people in any country can make perfect copies. Organized crime has entered the lucrative business of manufacturing and selling counterfeit software, CDs, and DVDs in a variety of countries, including Russia and Malaysia [13].

The second advance was the creation of the MP3 standard for compressing audio signals. A compression algorithm reduces the number of bits needed to store a picture or sound. An MP3 music file is typically less than 10 percent the size of the original file, but it is difficult to hear the difference between the original and the compressed versions. The introduction of MP3 made it practical for people to exchange music over the Internet.

The third technological advance was the increase in the number of people with high-speed Internet connections. While a patient person with an ordinary dial-up connection to the Internet can download large files, connections that are dozens of times faster make file sharing much more practical. As more people got DSL or cable access to the Internet, the number of downloads soared [2].

New Restrictions on Use

Legal and technological initiatives are restricting the ability of consumers to use CDs and DVDs, even for purposes that were previously considered fair use, such as making a backup copy. Larry Kenswil of Universal Music Group says, "What we really want to do is not to stop copying, simply to stop redistributing. But the technology available doesn't distinguish between the two"

Digital Millennium Copyright Act

The Digital Millennium Copyright Act (DMCA), passed by Congress in 1998, was the first major revision of United States copyright law since 1976. The primary purpose of the DMCA was to bring the United States into compliance with international copyright agreements it had signed Provisions in the DMCA significantly curtail fair use of copyrighted material. For example, the DMCA makes it illegal for consumers to make copies of any digitally recorded work for any purpose. It is illegal to sell (or even discuss online) a software program designed to circumvent copy controls [2].

Online service providers that misuse copyrighted materials face severe penalties. That means, for example, a university that knows students are exchanging MP3 files on the campus network and does nothing to stop them can be sued.

The DMCA extends the copyright protection to music broadcast over the Internet. It requires royalty payments to be made to copyright holders of music played over the Internet since October 1998. For example, a college Internet radio station would pay the larger of an annual fee of $500 or $0.0002 per listener per song for every song that it plays. Radio stations are having a hard time determining how much they owe, because most of them have not kept track of how many online listeners they have or the number of songs they have played [2].

Digital Rights Management

Digital rights management (DRM) can refer to any of a variety of actions owners of intellectual property may take to protect their rights. As Christopher May puts it, "all DRM technologies are aimed at tracking and controlling the use of content once it has entered the market" [2]. DRM technologies may be incorporated into a computer's operating system, a program, or a piece of hardware.

One approach to DRM is to encrypt the digital content so that only authorized users can access it. Another approach is to place a digital mark on the content so that a device accessing the content can identify the content as copy-protected.

🏋 Self Assessment 1-5

1. Patents are more likely to be granted to applications

1. describing a process of nature
2. describing mathematical algorithms
3. describing inventions
4. that manipulate data representing measurements made in the real world
5. I & II only
6. I & III only
7. II & III only
8. III & IV only
9. II, III & IV only

2. An idea may be protected by

1. Copyright
2. Trade secret
3. Patent
4. Trade mark

a. I & II only

b. II & III only

c. III & IV only

d. I & III only

e. I & IV only

3. In order for a company to maintain its right to a trade secret, it must

1. bind employees with non-disclosure agreements.
2. Protect its trademarks
3. Give up its copyright protection
4. Have it registered
5. I & II only
6. I & III only
7. II & III only
8. I & IV only
9. I only

4. The confidentiality of trade secrets may be broken through

1. the use of “clean room” software development strategy.
2. Reverse engineering
3. Hiring of former employees
4. I & II only
5. I & III only
6. II & III only
7. I, II & III
8. I only

5. With \_\_\_\_\_\_\_ one does not have to register his/her idea with the government in order to receive protection.

I. Patent

II. Trade mark

III. Copyright

IV. Service mark

1. I, II & IV only
2. I, III & IV only
3. II, III & IV only
4. II & IV only
5. III only

SESSION 2-5: PROTECTION FOR PROPRIETY SOFTWARE & OPEN SOURCE SOFTWARE

# 2-5.1 Software Copyrights

In the early days of the computer industry, there was no strong demand for intel­lectual property protection for software. Most commercial software was produced by the same companies manufacturing computer hardware. They sold complete systems to customers, and the licensing agreements covered use of the software as well as the hardware. Interest in copyrighting software grew with the emergence of an independent software industry in the 1960s.

The first software copyrights were applied for in 1964. The Copyright Office allowed the submitted computer programs to be registered, reasoning that a computer program is like a "how-to" book. The Copyright Act of 1976 explicitly recognizes that software can be copyrighted.

In 1980 the US congress passed the Computer Software Copyright Act, which clearly provides protection for registered software programs. It also sets forth the right of the purchasers to use the software while the creator retains legal title.

Copyright protection is explicit and clear-cut. It protects against copying of entire programs or their parts. Damages and relief are readily obtained for infringement. The drawback to copyright protection is that **the underlying ideas are not protected, only their manifestation in a work.** A competitor can use your software, understand how it works, and build his or her own software that follows the same concept without infringing on copyright. For example, suppose you develop a program for a relational database management system. You may be able to copyright your implementation of a relational database management system (your program), but you cannot copyright the concept of using relational databases to store information.

The main controversy with copyright is about the distinction between an idea and its expression. For instance, in the early 1990s Apple Computers sued Microsoft Corporation and Hewlett-Parker Inc. for infringement of the expression of Apple Macintosh interface. Among other claims, Apple claimed that the defendant copied the expression of overlapping windows. The defendant counter-claimed that the idea of overlapping windows can be expressed in only a single way and therefore was not protectable under the “merger” doctrine of copyright law. When ideas and their expression merge, the expression cannot be copyrighted. In general the court seems to be following an earlier court ruling where the elements of software had been dissected. The court found that neither similar concepts, functions, general functional features (e.g. drop-down menus), or colors are protect able by copyright law.

Second, copyright usually protects the object (executable) program, not the source program. Typically, the source code to a program is confidential, in other words, a trade secret of the enterprise that developed it. The company only distributes the object program to its customers. The copyright also protects the screen displays produced by the program as it executes. This is particularly valuable for the developers of video games.

Violations of Software Copyrights

The holder of a copyright has a right to control the distribution of the copyrighted material. Obviously, this includes making copies of the program. The definition of what it means to make a copy of a program is broad. Suppose you purchase a program stored on a CD. If you transfer a copy of the program from the CD to a hard disk, you are making a copy of it. If you execute the program, it is copied from the hard disk of the computer into its random access memory (RAM). This, too, is considered making a copy of the program. The standard licensing agreement that comes with a piece of commercial software allows the purchaser of the product to do both of the above-mentioned copying operations.

However, doing any of the following actions without authorization of the copyright holder is a violation of copyright law:

1. Copying a program onto a CD to give or sell to someone else

2. Preloading a program onto the hard disk of a computer being sold

3. Distributing a program over the Internet

# 2-5.2 Software Patents

Until the early 1980s, the U.S. Patent and Trademark Office refused to grant patents for computer software. Its position was that a computer program is a mathematical algorithm, not a process or a machine.

However, a U.S. Supreme Court decision in 1981 forced the Patent and Trademark Office to begin considering software patents. In the case of *Diamond v. Diehr,* the Supreme Court ruled that an invention related to curing rubber could be patented. Even though the company's principal innovation was the use of a computer to control the heating of the rubber, the invention was a new process for rubber molding, and hence patentable [2].

After this decision, the Patent and Trademark Office began reviewing applications for software patents. In each case, it needed to sort out applications merely describing mathematical algorithms from those describing inventions.

One way the distinction can be made is by looking at the data manipulated by the program. If the software simply manipulates values, such as a program that sorts numbers, it is an expression of a mathematical algorithm and should not be patented. On the other hand, if the software manipulates data representing measurements made in the real world, it is more likely to be a patentable invention. An example of such a piece of software would be a program inside a pacemaker that interprets electrocardiograph signals and determines when to administer an electric shock to the heart.

One problem faced by patent examiners in the Patent and Trademark Office is knowing what the existing technical knowledge (prior art) in computer programming is. Patent examiners typically look at patents already issued to determine prior art. This works fine for other kinds of inventions, but it doesn't work well for software patents, because a significant amount of software was written before software patents were first granted. The consequence is that patent examiners issue many "bad patents"- patents that would not have been issued if the examiner knew about all of the prior art. While organizations such as the Software Patent Institute are trying to collect information about prior art for patent examiners to use, the Patent and Trademarks Office continues to issue bad patents.

Bad patents can lead to increased legal costs for software companies. A software developer accused of patent infringement by another firm holding a bad patent must do its own research into the prior art to demonstrate the patent is invalid. Also, the existence of bad patents makes software patents in general more suspect. A general skepticism about the validity of software patents increases the likelihood that the owner of a software patent will have to defend challenges to the patent mounted by another software developer.

Safe Software Development

An organization must be careful not to violate the copyrights held by its competitors. Even unconscious copying can have serious consequences. Suppose a company needs to develop a software product that duplicates the functionality of a competitor's product without violating the competitor's copyright. For example, in the 1980s companies developing IBM-compatible computers needed to develop their own implementations of the BIOS (Basic Input/Output System). A "clean room" software development strategy helps ensure a company's software program does not duplicate any code in another company's product.

In this strategy, two independent teams work on the project. The first team is responsible for determining how the competitor's program works. It may access the program's source code, if it is available. If it cannot get access to the source, it may disassemble the object code of the competitor's product. It also reads the product's user manuals and technical documentation. The first team produces a technical specification for the software product. The specification simply states how the product is supposed to function. It says nothing about how to implement the functionality.

The second team is isolated from the first team. Members of this team have never seen any code or documentation from the competitor's product. It relies solely on the technical specification to develop, code, and debug the software meeting the specification. By isolating the code developers from the competitor's product, the company developing the competing product can demonstrate that its employees have not copied code, even unconsciously.

# 2-5.3 Consequences of Proprietary Software

In the early years of commercial computing, there was no independent software industry. Computer manufacturers such as IBM produced both the hardware and software needed for systems to be useable. Well into the 1960s, the software distribution included the source code. Customers who wanted to fix bugs in the programs or add new features could do so by modifying the source code and generating a new executable version of program.

In the I970s the number of computer applications expanded, and organizations organized the increasing value of software. To protect their investments in software development, most companies decided to make their programs proprietary (owned).

Today, companies developing proprietary software tightly control the distribution of their intellectual property. Typically they do this by treating source code as a trade secret and distributing only the object code, which is not in human-readable form. In addition, they do not sell the object code. Instead, when people "purchase" the program, what they are actually buying is a license allowing them to run the program. Their rights to do other things with the code, such as make backup copies, are limited.

*Governments* have given ownership rights to those who produce computer software because of the perceived beneficial consequences. A key benefit is the ability to profit from the licensing of the software. The assumption is that people will work harder and be more creative if they must compete with others to produce the best product. Those who produce the best products will have the opportunity to make money from them.

While most people point to the benefits of a system encouraging the development of proprietary software, some people have noted the harms caused by such a system. A well-known critic of proprietary software is Richard Stallman. According to Stallman, granting intellectual property rights to creators of computer software has numerous harmful consequences:

The copyright system was designed for an era in which it was difficult to create copies. Digital technology has made copying trivial. In order to enforce copyrights in the digital age, increasingly harsh measures are being taken. These measures infringe on our liberties.

The purpose of the copyright system is to promote progress, not to make authors wealthy. Copyrights are not promoting progress in the computer software field.

It is wrong to allow someone to "own" a piece of intellectual property. Granting someone this ownership forces the users of a piece of intellectual property to choose between respecting ownership rights and helping their friends. When this happens, the correct action is clear. If a friend asks you for a copy of a proprietary program, *you* would be wrong to refuse your friend. "Cooperation is more important than copyright"

The open-source movement holds the philosophical position that source code to software ought to be freely distributed and that people should be encouraged to examine and improve each other's code. The open-source software movement promotes a cooperative model of software development.

# 2-5.4 Open-Source Definition

Open source is an alternative way of distributing software. Licenses for open-source programs have the following key characteristics (there are others) [14]:

1. There are no restrictions preventing others from selling or giving away the software.

2. The source code to the program must be included in the distribution or easily available by other means (such as downloadable from the Internet).

3. There are no restrictions preventing people from modifying the source code, and derived works can be distributed according to the same license terms as the original program.

4. There are no restrictions regarding how people can use the software.

5. These rights apply to everyone receiving redistributions of the software without the need for additional licensing agreements.

6. The license cannot put restrictions on other software that is part of the same distribution. For example, a program's open-source license cannot require all of the other programs on the CD to be open source.

Note there is nothing in these guidelines that says an open-source program must be given away for free. While people may freely exchange open-source programs, a company has the right to sell an open-source program. However, a company cannot stop others from selling it either. In order for a company to be successful selling open-source software that people can find for free on the Internet, it must add some additional value to the software. Perhaps it packages the software so that it is particularly easy to install. It may provide great manuals, or it may provide support after the sale.

The Open Source Initiative (www.opensource.org) is a nonprofit corporation that promotes a common definition of open source.

# 2-5.5 Beneficial Consequences of Open-Source Software

Advocates of open-source software describe five beneficial consequences of open-source licensing.

The first benefit of open source is that it gives everyone using a program the opportunity to improve it. People can fix bugs, add enhancements, or adapt the program for entirely new uses. Software evolves more quickly when more people are working on it.

Rapid evolution of open-source software leads to the second benefit: new versions of open-source programs appear much more frequently than new versions of commercial programs. Users of open-source programs do not have to wait as long for bug fixes and patches.

A third benefit of open source is that it eliminates the tension between obeying copyright law and helping others. Suppose you legally purchased a traditional license to use a program, and your friend asks you for a copy. You must choose between helping your friend and conforming to the license agreement. If the program had an open-source license, you would be free to distribute copies of it to anyone who wanted it.

The fourth benefit is that open-source programs are the property of the entire user community, not just a single vendor. If a vendor selling a proprietary program decides not to invest in further improvements to it, the user community is stuck. In contrast, a user community with access to the source code to a program may continue its development indefinitely

The fifth benefit of open source is that it shifts the focus from manufacturing to service, which can result in customers getting better support for their software. As Eric Raymond puts it:

Anybody who has studied software engineering knows that programmers do not actually spend most of their time originating software. They spend most of their time on service updates and maintenance. Nobody thinks about the implications of this: that the software industry is actually a service industry operating under the delusion that it is a manufacturing industry. Software producers are operating under a manufacturing model, under which the way you make money is building a product and getting it out the door. Because they have this model of themselves as a manufacturing industry, all the bright people go to production and the dumb people go to the support desk. That's why when you call a vendor support line you have to fight your way through three layers of idiots to get down to anyone who knows anything.

As long as the software industry continues to misperceive itself as a manufacturing industry, instead of a service industry, reliability is going to be awful. But that shift is not going to happen until source is open. That's the difference between closed and open source.

In the closed source world, your short-term profit incentive is to try and keep everything you do a trade secret and extract the absolute maximum rent from that trade secret in terms of initial cost of the software. And then your economic incentive is to put as little money as you can get away with into supporting the fiction that you support your software. OK? Now as a consumer do you want to live in that world, or do you want to live in a world where source is primarily open and the people competing for your dollars are service bureaus?

Examples of Open-Source Software

Open-source software is a key part of the Internet's infrastructure. Here are a few examples of highly successful programs distributed under open-source licenses:

* BIND provides DNS (domain name service) for the entire Internet.
* Apache runs more than half of the world's Web servers
* The most widely used program for moving email about the Internet is the open source program sendmail.
* Perl is the most popular Web programming language.
* Other popular open-source programming languages and tools are Python, Ruby, TCL/TK, PHP, and Zope.
* Programmers have recognized the high quality of the GNU compilers for C, *C++,* Objective-C, FORTRAN, Java, and Ada.

Surveys indicate that the quality and dependability of open-source software is about the same as the quality of commercial software [2].

🏋 Self Assessment 2-5

1. Software copyright protects

1. Source code
2. Object code
3. Screen displays
4. Design specifications
5. I & II only
6. I & III only
7. II & III only
8. III & IV only
9. I, II & III only

2. If you “purchase” proprietary software stored on a CD, you have the right to

1. Preload the software onto the hard disk of a computer you are selling if the computer too is yours.
2. Transfer a copy of the software from the CD to a hard disk of your computer.
3. Copy the software from the hard disk to the RAM of your computer for execution.
4. Copy the software onto another CD to give free to a friend
5. I & III only
6. I & II only
7. II & III only
8. III & IV only
9. II, III & IV only

3. Today when you “purchase” proprietary software,

1. You receive only the object code, which is not in human-readable form.
2. You are restricted on the number of copies you can make as backup.
3. You can improve on the software under “fair use”.
4. You actually buy a license allowing you to run the program.
5. I & II only
6. I & IV only
7. II & III only
8. I, III & IV only
9. I, II & IV only

4. Open source programs

1. cannot be sold.
2. Can be modified and given to others under the same licensing terms as the original program.
3. Can be used in anyway one find appropriate.
4. I & II only
5. I & III only
6. II & III only
7. I, II & III
8. I only

5. In order to be successful selling open-source software that people can find for free on the internet, one may have to

1. Provide great manuals
2. Provide after sales service
3. Package the software so that it is particularly easy to install
4. Include the source code to the program or be easily downloaded from the internet.
5. I & II only
6. I & III only
7. II & III only
8. I, II, & III only
9. I, II, III & IV

 *Learning Track Activities*

|  |  |
| --- | --- |
| j0299125 | Unit Assignments 5  1. Explain how advances in IT have made it easier for consumers to violate copyright law.  2. Why are patents considered an unreliable way of protecting intellectual property rights in software?  3. To determine fair use, what factors need to be considered?  4. When describing software license, what does the phrase “Open Source” mean?  5. What are the beneficial consequences of Open-Source software? |
|  |  |

Unit 6

COMPUTER RELIABILITY, EMPLOYMENT & WORK

Introduction

Many of our activities are tracked by computers, and information about us are kept on computer databases. What happens when a computer is fed with bad information, or when someone misinterprets the information they retrieve from the computer? What happens when an embedded computer in a device fails due to perhaps a software error?

The effects of some computer errors, such as a game doing something unusual or even crashing when playing a computer game, are trivial. Sometimes the result of a computer malfunction may result in real inconvenience such as receiving an incorrect bill and you having to spend a couple of hours on the phone to have it corrected. Some businesses have made poor decisions which have cost them millions of dollars due to software bugs they had on their system. On a few occasions, failures in a computerized system have even resulted in fatalities.

In this unit we start by discussing who should be held accountable and therefore held liable for harm done to people because of for example software errors?

We then move on to examine various ways in which computerized systems have proven to be unreliable. Systems typically have many components, of which the computer is just one. A well engineered system can tolerate the malfunction of any single component without failing. Unfortunately, there are many examples of systems in which the computer was the weakest link and a computer error lead to the failure of the entire system. The failure may have been due to data-entry or data-retrieval error, poor design or inadequate testing.

The negative social costs of introducing Information System and Information Technology are beginning to mount along with the power of the technology. Many of these negative social consequences are not violations of individual rights, nor are they property crimes. Nevertheless, these negative consequences can be extremely harmful to individuals, societies and political institutions. Computers and Information Technologies potentially can destroy valuable elements of our culture and society even while they bring us benefits. If there is a balance of good and bad consequences to the use of IT, who do we hold responsible for the bad consequences? At the final session of this unit we examine some the negative consequences of IT and Information System.

We discuss some of the many changes that Information Technology and automation have brought to the workplace and we ask questions such as, Has automation brought unemployment? Some evidence support an affirmative answer to the question, but other evidence suggests that automation actually creates more jobs than it replaces.

We describe how IT has lead to significant changes in the way companies organize themselves and increases in telework, and workplace monitoring. We then take a look at various maladies that are as a result of the introduction and use of IT.

Many in developed countries view those without access to IT as being severely disadvantaged. The term “digital divide” refers to the opportunity gap brought about because some people do not have access to modern IT, particularly the Internet. We examine the issue of digital divide and the effects that IT is having on the traditional boundaries that separate work from family and leisure.

|  |  |
| --- | --- |
| j0293844 | Learning Objectives  After reading this unit you should be able to:   1. Appreciate the challenges of accountability, liability, and control that new IT brings to bear on existing laws and social practices. 2. Describe the principal sources of poor system performance. 3. Explain the importance of effects of computers on the work environment and health 4. Explain the implications of IT for employment and the future. |

Unit content

**Session 1-6: Computer Reliability**

1-6.1 Accountability, Liability, And Control

1-6.2 Data Quality And System Errors

1-6.3 Poor Software Performance Due To Software Bugs And Errors

1-6.4 Software System Failures

1-6.5 Data-Entry Or Data–Retrieval Errors

**Session 2-6: Employment, Work And Health Concerns**

2-6.1 Employment And Job Losses

2-6.2 Work Place Changes

2-6.3 Health Concerns

2-6.4 Other Concerns

SESSION 1-6: Computer Reliability

# 1-6.1 Accountability, Liability, And Control

Along with privacy and property laws, new Information Technologies are challenging existing law and social practices for holding individuals and institutions accountable. If a person is injured by a machine controlled by software, who should be held accountable and therefore held liable? Should a public bulletin board or an electronic service like Prodigy or CompuServe permit the transmission of pornographic or offensive material (as broadcasters), or should they be held harmless against any liability for what users transmit (as is true of common carriers like telephone services)? What about the Internet? If you outsource your information processing, can you hold the external vendors liable for injuries done to your customers? Let’s look at some liability problems.

On March 13, 1993, a blizzard hit the east coast of the United States, knocking out an EDS (Electronic Data System Inc.) computer centre in Clifton, New Jersey. The centre operated 5,200 automatic teller machines in 12 different networks across the country involving more than one million card holders. In the two weeks required to recover operations, EDS informed its customers to use alternative ATM networks operated by other banks or computer centres and offered to cover more than $50 million in cash withdrawals. Because the alternative networks did not have access to the actual customer account balances, EDS is at substantial risk of fraud. Cash withdrawals were limited to $100 per day per customer to reduce the exposure. Most services were restored by March 26. Although EDS had a disaster recovery plan, it did not have a dedicated backup facility. In this case, who is liable for any economic harm caused individuals or businesses that could not access their full account balances in this period [1]?

In April 1990, a computer system at Shell Pipeline Corporation failed to detect a human operator error. As a result, 93,000 barrels of crude oil were shipped to the wrong trader. The error cost $2 million because the trader sold oil that should not have been delivered to him. A court ruled later that Shell Pipeline was liable for the loss of the oil because the error was due to a human operator who entered erroneous information into the system. Shell was held liable for not developing a system that would prevent the possibility of misdeliveries [1]. Who would you have held liable – Shell Pipeline? Is it the trader for not being more careful about deliveries? Or is it the human operator who made the error?

Information Systems executives who are ultimately responsible for the harm done by systems developed by their staffs face great difficulties. In general, in so far as computer software is part of a machine, and the machine injures someone physically or economically, the producer of the software and the operator can be held liable for damages. In so far as the software acts more like a book, storing and displaying information, courts have been reluctant to hold authors, publishers, and booksellers liable for content ( the exception being instances of fraud and defamation), and hence courts have been wary of holding software authors liable for “book-like” software regardless of the physical or economic harm that results. It was feared that liability claims would interfere with their rights of expression.

Software that provide service, such as automatic teller machines if they should fail, bring considerable inconvenience and perhaps economic harm to bank customers if they cannot access the funds in a timely manner. The question is; should liability protections be extended to software publishers and operators of defective financial, accounting, simulation, or marketing system?

Software is very different from books. Software users may develop expectations of infallibility about software; software is less easily inspected than a book and more difficult to compare with other software products for quality; and software claims actually to perform a task rather than describe a task like a book. People come to depend on services essentially based on software. Given the centrality of software on everyday life, the chances are excellent that liability laws will extend its reach to include software even when it merely provides an information service.

# 1-6.2 Data Quality And System Errors

The debate over liability and accountability for unintentional consequences of system use raises a related but independent moral dimension: What is an acceptable, technologically feasible level of system quality. Individuals and organizations may be held responsible for avoidable consequences – foreseeable consequences – which they have a duty to perceive and correct. But some system errors are foreseeable and correctable only at very great expenses, an expense so great that pursuing this level of perfection is not feasible economically – no one could afford the product. For example, although software companies try to debug their products before releasing them for sale, they knowingly ship buggy products because the time and cost to fix all minor errors would prevent these products from ever being released. What would be the effect on society if the product was not released at all? The question is, should the producer withdraw the product that can never be perfect, warn the user, or forget about the risk (let the buyer be ware)?

Three principal sources of poor system performance are software bugs and errors, hardware or facility failures due to natural causes, and poor input data quality due to improper procedures. Despite many people’s distrust, computers themselves rarely make mistakes. Even the most sophisticated hardware cannot produce meaningful output if users do not follow proper procedures. Mistakes can be caused by unclear expectations and a lack of feedback or a programmer might develop a program that contains errors. In other cases, a data-entry clerk might enter the wrong data. Unless errors are caught early and prevented, the speed of computers can intensify mistakes. A discussion of the principal sources of poor system performance follows next.

# 1-6.3 Poor Software Performance Due To Software Bugs And Errors.

Software code of any complexity cannot achieve zero defects and the seriousness of remaining bugs cannot be estimated. Hence, there is a technological barrier to perfect software, and users must be aware of the potential for catastrophic failure. The software industry has not yet arrived at testing standards for producing software of acceptable but not perfect performance.

Let’s take a look at some computer-related mistakes:

On July 21, 2001, Linda Brooks of Minneapolis, Minnesota received a phone bill of $57,346.20. Some customers of the telephone company had been billed as much as $600.00 per minute for use of their mobile phones. 14,000 customers received incorrect bills and this was due to a bug in the telephone company’s newly installed billing system [2].

In 1996, a software error at the U.S. Postal Service caused it to return to the senders two weeks’ worth of mail addressed to the Patent and Trademark Office. In all 50,000 pieces of mail were returned to sender [15].

On the morning of March 1, 2003, Japan’s air traffic control system went down for an hour, delaying departures for hours. The backup system failed at the same time as the main system, which was out of commission for four hours. Airports kept in touch via telephone, and no passengers were put at risk. However, some flights were delayed over two hours, and 32 domestic flights had to be cancelled [2].

Another example of a somewhat small error is the one a school employee in Newark, New Jersey, made in coding the school’s master scheduling program. When 1000 students and 90 teachers showed up for the start of school at Central High School, half the students had incomplete or no schedule for classes. Some classrooms had no teachers while others had four instead of one [10].

# 1-6.4 Software System Failures

Many modern devices contain embedded systems – a computer used as a component of a larger system. You can find microprocessor-based systems in microwave ovens, thermostats, automobiles, traffic lights, and a myriad of other modern devices. Because every computer needs software to execute, every embedded system has a software component.

Software is playing an ever-larger role in system functionality. There are several reasons why hardware controllers are being replaced by microprocessors controlled by software. Software controllers are faster. They can perform more sophisticated functions, taking more input data into account. They cost less, use less energy, and do not ware out. Unfortunately, while hardware controllers have a reputation for high reliability, the same cannot be said of their software replacements.

Most embedded systems are also real-time systems: computers that process data from sensors as event occur. The microprocessors that controls the air bags in a modern automobile is an example of a real time system , because it must instantly react to readings from its sensors and deploy the air bags at the time of a collision. The following are examples of embedded systems that have failed as a result of failures in their software components.

In May, 2003, a space mission ended in a wild ride with the American and Russian crew going some 250 miles off course due to a computer error. A computer malfunction sent the capsule’s occupants on such a steep reentry trajectory that their tongues rolled back in their mouths. Indeed the landing was so far off target that more than two gut-wrenching hours passed before the recovery team knew the men were safe [9].

The Patriot missile system was originally designed by the U.S. Army to shoot down air-planes. In the 1991 Gulf War, the Army put the Patriot missile system to work, defending against Scud missiles launched at Israel and Saudi Arabia. Later analysis revealed that, perhaps as few as 9 percent of the scuds were actually destroyed by scud missiles and that the Patriots missile defence system was not 95 % effective as earlier claimed. Rather many scud missiles fell apart as they approached their target – their destruction had nothing at all to do with the Patriot missiles launched at them [2].

On the afternoon of January 15, 1990, AT&T’s long-distant network suffered a significant disruption of service. About half of the computerized telephone-routing switches crashed, and the remainder of the switches could not handle all of the traffic. As a result of this failure, abour 70 million long-distance telephone calls could not be put through, and about 60,000 people lost all telephone service. AT&T lost tens of millions of dollars of revenue. It also lost some of its credibility as a reliable provider of long-distance service [2].

# 1-6.5 Data-Entry Or Data–Retrieval Errors

While software bugs and facility catastrophe are likely to be widely reported in the press, by far the most common source of business system failure is data quality. A total of 70% of Information System executives in a survey reported data accuracy was unacceptable and 44% said no systems were in place to check database information quality. Consider the following reported cases of data quality problems [1].

A Japanese company, Catena Corporation, was deluged with thousands of orders for over 100 million Apple Computer Inc. EMac computers after a glitch caused the computers to be listed on an online shopping site for a price of $25.45. The company said a code number assigned to a set of five 8X DVD-R discs, which were the products it was intending to sell, was sent to Yahoo! Japan; however, a product information database matched that code details for the eMac computer and with the price for the DVDs. The result was a listing for the computer, part number M9461J/A, at a price of $25 rather than the usual price of more than $916 [16].

Amazon.com shut down its British Web site on March 13, 2003, after a software error led it to offer iPaQ handheld computers for £7 instead of the correct price of about £275. Before Amazon.com shut down the site, electronic bargain hunters had flocked the Amazon.com’s Web site, some of them ordering as many as ten iPaQs [2].

Several studies have established that 5-12 % of bar code sales at retail grocery and merchandise chains are erroneous and that the ratio of overcharges to undercharges runs as high as 5:1, with 4:1 as a norm. The problem tends to be human error in keeping shelf prices accurate and corporate policy that fails to allocate sufficient resources to price checking auditing, and development of error-free policies. The cause of the high overcharge has not yet been determined, but the pattern is disturbing, suggesting intentional behaviour. California Macy’s stores, for example, agreed to a $1.2 million settlement for overcharging shoppers in the city of San Diego, Los Angeles County, and three other counties. Investigators found that while all the company’s scanners were 100 percent accurate, consumers were being charged from a few cents to more than $10 over the advertised and shelf prices of some clothing and household items. The problem was traced to difficulty in synchronizing the advertised prices, the price on the shelf, and the price in the (checkout register) computer. No one alleged that Macy’s intentionally overcharged consumers, but the store “had a real pattern of inaccuracy all across the state,” according to the Los Angeles County prosecuting attorney [9].

A manufacturer attempted to reorganize its customer files by customer number only to discover that the sales staff had been entering a new customer number for each sale because of special incentives for opening new accounts. One customer was entered 7000 times. The company scrapped the software project after spending $1 million.

An airline inadvertently corrupted its database of passenger reservations while installing new software, and for months planes took off with half loads.

Thousands of patients of Kaiser Permanente Health Plan Incorporated may have received the wrong medication when its computer systems suffered a power outage that could have caused labelling errors on prescriptions dispensed to 4,700 patients. Patients could have received incorrect prescriptions numbers, incorrect instructions about how to take the drug, or even the wrong drugs. Kaiser Permanente quickly contacted the affected patients via automated telephone calls, courier-delivered letters, and home visits. Fortunately there were no adverse patient reactions [9].

The databases of the National Crime Information Center (NCIC) contain a total of about 40 million records related to stolen automobiles, missing persons, wanted persons, suspected terrorists, and more. There have been numerous false arrests based on information they retrieved from the NCIC. Shiela Jackson Stossiet, an airline flight attendant, for example was arrested at the New Orleans airport by police who confused her with Shirley Jackson, who was wanted in Texas. She spent one night in jail and was detained for five days.

California police, relying upon information in the NCIC, twice arrested and failed Roberto Hernandez as a suspect in a Chicago burglary case. The first time he was jailed for 12 days, while the second time he was held for a week before he was freed. They had confused him with another Roberto Hernandez, who had the same height and weight. Both Hernandez had brown eyes, and tattoos on their left arms. They also had the same birthday, and their Social Security numbers differed by only a single digit.

🏋 Self Assessment 1-6

1. Some of the negative social consequences due to the introduction of Information Systems and Information Technology which are not violations of individual rights or property rights are

I. Millions of middle level managers and clerical workers are losing their jobs

II. More and more people are now working from home, thus weakening the family and other institutions

III. There is more occupational stress and disease due to IT.

IV. There is more hacking and Internet fraud.

1. I, II & IV only
2. I, III & IV only
3. II, III & IV only
4. I, II & III only
5. I & II only

2. Even though software acts more like a book, storing and displaying information, in what instances are courts likely to hold software developers liable for content?

I. Libel

II. Defamation

III. Deception

IV. Fraud

a. I and II only

b. I and III only

c. II and III only

d. III and IV only

e. II and IV only

3. Software controllers are replacing hardware controllers in modern embedded systems because software controllers \_\_\_\_\_\_\_\_.

I. cost less.

II. are more reliable.

III. use less energy.

IV. are faster

a. II only

b. II and III only

c. I, III and IV only

d. I, II and III only

e. I, II, III and IV

4. Controllers that process data sensors as events occur are known as \_\_\_\_\_\_\_\_\_\_ systems.

a. event sensor

b. sensor

c. embedded

d. automatic

e. real-time

5. Which of these is by far the most common source of business system failure?

a. Software bugs

b. Hardware failure

c. Data-entry error

d. Errors in standard operating procedures

e. None of the above

SESSION 2-6: Employment, Work And Health Concerns

# 2-6.1 Employment And Job Losses

Reengineering work is typically hailed in the Information System community as a major benefit of IT. It is much less frequently noted that redesigning business processes could potentially cause millions of middle level managers and clerical workers to loss their jobs. One economist has raised the possibility that we will create a society run by a small “high tech elite or corporate professionals in a nation of permanently unemployed” [1]. Some have estimated that if reengineering were seriously undertaken by the Fortune 1000 companies, about 25% of the U.S. labour force would be displaced. Reengineering has been seriously used at only 15% of American service and manufacturing companies, and the average reduction in employment in downsizing companies is 10% in a year [1]. However, the effect of reengineering may be growing, leaving management with a serious ethical dilemma.

Economists take the potential of job losses much lighter. They believe that relieving bright, educated workers from reengineering jobs will result in these workers moving to better jobs in fast-growing industries. Left out of this equation are blue collar workers and older, less-educated middle managers. It is not clear that these groups can be retained easily for high-quality (high paying) jobs.

Other observers hold a quite different view about the effect of automation and information technology on jobs. They have concluded that while new technology may destroy certain jobs, it also creates new jobs. The net result is an increase, not a decrease in the number of available jobs. Martin Carnoy points out that the absolute number of manufacturing jobs in the world is increasing, not decreasing. He writes “There will be plenty of jobs in the future, and most of them will be high-paying jobs” [2].

The logic of these “automation optimists” is that, on the surface, it is obvious that automation eliminates jobs. After all, that’s what automation means. However, it’s also important to look beneath the surface. Automation is introduced as a cost-saving measure: it is less expensive for a machine to perform a particular job than a human being. Because companies compete with each other, lower production costs result in lower prices for the customer. The drop in the price of a product has two beneficial effects. First, it increases the demand for the product. In order to produce more of the product, workers must be hired. Second, people who were already purchasing the product don’t have to pay as much for it. That gives them more money to spend on other things, increasing the demand for other products. This, too, results in job creation. Finally, there is an additional effect. Some people must be employed to design, create, and service the automation devices themselves [2].

Two studies commissioned by the International Labour Office has reached the same conclusion as Carnoy. While automation appears to reduce employment when particular factories or companies are examined, studies of entire industries and economies do not reveal job losses.

# 2-6.2 Work Place Changes

Experts debate whether or not IT has resulted in a net reduction in available jobs, but there is no dispute that IT has affected how people work. Here are a few ways that IT is fundamentally changing the work experience.

**Organizational Changes**

IT has influenced the way manufacturing and service companies organize themselves. A typical early use of computers was to automate a back-office function such as payroll. Using computers in this way required a company to make no changes in its organization. Later, companies began using computers inside manufacturing units. Computers enabled companies to customize products and provide better service to their customers. This use of computers delegated more responsibility to the line workers, and it encouraged a decentralization of sales and support functions, reducing a company’s bureaucracy. IT within corporations reached a third stage with the creation of computer networks linking different parts of the business. For example integrating cash registers with inventory systems has allowed companies to order replacements automatically.

The overall effect of the introduction of IT is to flatten organizational structures. When the primary source of information distribution was the hand-typed, carbon-copied memorandum, most information flow followed the lies in organizational charts. Today a wide variety of technologies allow any member of an organization to contact other members with minimal effort and cost. As a result, new opportunities arise. Many organizations assemble “tiger teams” of expert workers drawn from various parts of the organization chart. A team will work together for a short period of time to solve an urgent problem, and then disband. Flexible information flow also allows companies to adopt “just-in-time” production and distribution methods, reducing inventory costs. Today, many companies have adopted supply-chain automation, eliminating the need for middlemen. Automating the paperwork activities associated with purchasing supplies can reduce the number of people who produce purchase orders and invoices, pay bills, process cheques, etc. The likely effect of IT on organizations will be an increased demand in some job categories, while the demand in other categories will drop.

**Telework**

Another workplace change brought through IT is the rise of telework. Telework (also called telcommuting) refers to an arrangement where employees spend a significant portion of their work day at a distance from the employer or traditional work place of work. One kind of teleworking is working from a home office. Another example of teleworking is someone who commutes to a telecenter rather than the company’s site. Telecenters provide employees from different firms the ability to connect to their company’s computers. A third example of teleworking is salespersons who have no offices, instead transacting all of their business from their cars using cell phones and laptop computers. The number of people teleworking in developed countries is increasing rapidly.

Some of the advantages of telework are the following:

1. It increases productivity:- A variety of studies have shown that teleworkers have 10 to 43 percent more productivity than on-site workers.
2. It reduces absenteeism:- Teleworkers are less likely to miss work than someone commuting from home to the office.
3. It improves moral:- Tele workers have more freedom. It is easier for them to schedule their work around their personal schedules. They can also dress more casually and get on with the job.
4. A company can recruit and retain more employees:- Employees who otherwise would not be interested in the job because they are unable or unwilling to be within commuting distance of the main office, can recruit such people as teleworkers. It allows companies to retain employees (such as mothers of young children) who would quit otherwise.
5. It saves overhead:- With some of its workers away from the office, a company doesn’t have to invest as much in office accommodation.
6. It improves the resilience of a company:- The company is less likely to be harmed by a natural disaster or a terrorist attack because not all the employees are in one place.
7. It is good for the environment:- It reduces the amount of pollution caused bu commuting traffic.
8. Employees may save money by teleworking:- They may not have to purchase as much business attire, and may be able to avoid paying child-care expenses.

Some disadvantages of teleworking too are as follows:

1. It threatens the authority and control of managers:- Working at a distance from managers, employees naturally have more autonomy. How can a manager manage an employee who is not around?
2. It is impossible for an employee to have a face-to-face interaction with customers at the company site. For some jobs this interactions is crucial , meaning the job simply cannot be done from a distance.
3. Sensitive information is less secure:- Valuable physical or electronic files at home or in an automobile is far less secure than if they were kept in an office.
4. When people in an organization do not keep the same hours or come into the office everyday, it is more difficult to schedule meetings.
5. Teleworkers are less visible:- When somebody is “never around”, others can get the idea that that person is not making a contribution to the organization. Such teleworkers may be forgotten when it’s time for pay raises and promotions.
6. When faced with a problem or a need for information, employees at the office are less likely to contact a teleworker than another person on site.
7. Teleworkers are isolated:- Some jobs require people to bounce ideas of co-worker. With no co-workers around, what are teleworkers suppose to do?
8. Teleworkers end up working longer hours for the same pay because everything they need to work with is available and they keep going back to the job at ever spare time they get.

**Monitoring**

Currently, the right of workers who want their privacy and the interest of companies that demand to know more about their employees are in conflict. Recently companies have been monitoring their workers via computer technology. These computer-monitoring systems tie directly into workstations; specialized computer programs can track every keystroke made by the user. This type of system can determine what workers are doing while at the keyboard. The system also knows when the worker is not using the keyboard or computer system and can even take snapshots of employees computer monitors. These systems can estimate what a person is doing and how many breaks he or she is taking. Needles to say, many workers consider this close supervision very dehumanizing.

When using your *e-mail at work* do you think that your boss cannot snoop on your e-mail? The law allows employers to “intercept” employee communication if one of the parties involved agrees to the interception. The party involved in this case is the employer. Indeed, employer snooping seems to be widespread. Thus a good rule of thumb, suggest one writer, is to “think of an e-mail message not as a sealed letter but as a postcard – and, even more a postcard that might well be read and copied in every post office it passes through, then kept on file for years after”.

Other examples of employee monitoring include tracking Internet usage, monitoring phone calls, reviewing computer files, and videotaping.

Monitoring can serve many purposes. The principal purpose of monitoring is to identify inappropriate use of company resources. For example, the use of the company’s Internet for surfing the Web for pornography and time used in reading and sending email the contain gossip and jokes. Monitoring can help detect illegal activities even by monitoring instant messaging conversations. Monitoring can also be used to ensure that customers are getting the products and services they need.

The question however is whether monitoring is ultimately beneficial to an organization or not. Obviously organizations institute monitoring because they have reason to believe it will improve the quantity and/or quality of the work performed by its employees. There is evidence that employee monitoring makes employees more focused on their tasks, but also reduces job satisfaction.

**Globalization**

Globalization refers to the process of creating a worldwide network of businesses and markets. Globalization results in a greater mobilization of goods, services, and capital around the world. Investments are made across national boundaries. Products manufactured in one country are sold in another. Consumers calling a telephone help center get connected with support technicians located on the other side of the world.

The rapidly decreasing cost of IT has made globalization possible. The cost of computing dropped by 99.99 percent between 1975 and 1995 [2]. The cost of telephone calls also dropped by similar magnitudes. Companies have made extensive use of low-cost IT to coordinate operations distributed around the planet.

# 2-6.3 Health Concerns

For some people, working with computers can cause occupational stress. Anxieties about job insecurity, loss of control, incompetence, and demotion are just a few of the fears workers might experience. In some cases, the stress may become so sever that workers may sabotage computer systems and equipment. Monitoring employees stress may alert companies to potential problems. Training and counselling can often help the employees and deter problems.

Computer use may affect physical health as well. According to the Joyce Institute in Seattle, U. S., strains, sprains, tendonitis, and other problems account for more than 60 percent of all occupational illness and about a third of workers’ compensation claims. The cost to U. S. corporations for these types of health problems is as high as $27 billion annually [1].

The most important occupational disease today is repetitive stress injury (RSI), representing 56% of all workplace maladies. RSI (also known as Repetitive Motion Disorder) occurs when muscle groups are forced through the same repetitive actions often with high-impact loads (like tennis) or tens of thousands of repetitions under low-impact loads (like working at a computer keyboard) [1].

The single largest source of RSI is computer keyboards. Forty-six million Americans use computers at work, and 185,000 cases of RSI are reported each year, according to The U. S. National Center for Health Statistics. The most common kind of computer-related RSI isCarpal Tunnel Syndrome (CTS), in which is the aggravation of the pathway for nerves that travel through the wrist bone structure (the carpal tunnel) produce pain. The aggravation is caused by a number of factors, such as stress, lack of exercise, and the repetitive motion of typing on a computer keyboard. In a single shift, a word processor may perform 23,000 keystrokes. Symptoms of CTS include numbness, shooting pain in the wrist, inability to grasp or hold objects, and tingling.

RSI is avoidable. Designing workstations for a neutral wrist position (using a wrist rest to support the wrist), proper monitor stands, and footrest all contribute to proper posture and reduced RSI. New ergonomically correct keyboards are an option, although their efficacy has yet to be clearly established. These measures should be backed up by frequent rest breaks, rotation of employees to different jobs, and moving towards voice and scanner data entry. RSI is not the only occupational illness caused by computers: back and neck pain, leg stress, and foot pain also result from poor ergonomics designs of workstations.

Other work-related health hazards involve emissions from improperly maintained and used equipment. Some studies show that poorly maintained laser printers may release ozone into the air; others dispute the claim.

Computer Vision Syndrome (CVS) refers to any eye strain condition related to computer display screen use. Its symptoms are headaches, blurred vision, and dry irritated eyes, but these symptoms are usually temporal. Numerous studies on the impact of emissions from display screens have also resulted in conflicting theories. Although some medical authorities believe that long-term exposure can cause cancer, studies are not conclusive at the moment.

Video display terminals (VDT) emit non-ionizing electric and magnetic fields at low frequencies. These rays enter the body and have unknown effects on enzymes, molecules, chromosomes, and cell membranes. Early studies suggesting a link between low-level EMFs (Electromagnetic Fields) and miscarriages have been contradicted by later, superior study published in 1991 .

Most computer manufactures publish technical information on radiation emission from their screens, and many companies pay close attention to this information. All manufacturers have reduced display screen emissions since the early years of the 1980’s and European countries like Sweden have adopted very stiff radiation emission standards. San Francisco was one of the first cities to propose a video display terminal (VDT) bill. The bill requires companies with 15 or more employees who spend at least four hors a day working with computer screens to give 15-minute break every 2 hours. In addition, adjustable chairs and workstations are required if employees request them.

The newest computer-related malady is **technostress**, defined as a computer use-induced stress whose symptoms are irritation, hostility towards humans, impatience, and enervation. The problem according to experts is that humans working continually with computers come to expect other humans and human institutions to behave like computers, providing instant response, attentiveness, and with an absence of emotion. Computer-intense workers are irritated when put on hold during a phone call, become incensed or alarmed when their PCs take a few seconds longer to perform a task, lack empathy for humans, and seek friends who mirror the characteristics of their machines. Technostress is thought to be related to high levels of job turnover in the computer industry, high levels of early retirement from computer-intense occupations, and elevated levels of drug and alcohol abuse [1].

The World Health Organization (WHO), U. S. Food and Drug Administration (FDA), and the U. S. General Accounting Office (GAO) have also analyzed health data on cell phone use, but they cannot definitively say whether cell phones pose any health risk.

# 2-6.4 Other Concerns

**The Digital Divide**

Does everyone have an equal opportunity to participate in the digital age? Will the social, economic, and cultural gaps that exist in our society be reduced by Information Systems technology? Or will the cleavages be increased, permitting the “better off” to become still better off? When and if computers become everywhere will it include the poor as well as the rich? The digital divide refers to the situation where some people have access to modern IT while others do not.

The answers to these questions are clearly not known, as the differential impact of systems technology on various groups in society has not been well studied. What is known is that information and knowledge, and access to these resources through educational institutions and libraries, are inequitably distributed. Access to computers is distributed inequitably along social class lines, as are many other information resources. If this situation is left uncorrected, we could end up creating a society of information haves, computer literates and skilled, versus a large group of information have-nots, computer illiterates and unskilled.

It is worth noting however that the digital divide has two fundamentally different dimensions. The global divide refers to the disparity in Internet access between more industrialized and less industrialized nations. The social divide refers to the difference in access between the rich and poor within a particular country.

**Maintaining boundaries: family, work, leisure**

The traditional boundaries that separate work from family and just plain leisure are being weakened. The advent of Information System coupled with the growth of knowledge work occupation, means that more and more people will be working, when traditionally they would have been playing or communicating with family and friends. The “work-umbrella” now extends far beyond the eight-hour day.

Weakening these institutions poses clear-cut risks. Family and friends historically have provided powerful support mechanisms for individuals and they act as balance points in a society by preserving “private life”, providing a place for one to collect one’s thoughts, think in ways contrary to one’s employer, and to dream.

The question then is what lessons can we in a developing country like Ghana draw from this? Are we going to wait until there is complete anarchy as far as the use of IT is concerned or there has been real harm before parliament acts, or are we going to take advantage of the experiences of countries such as the United States, United Kingdom, Australia, etc, who have walked that same path, made mistakes and rectified the situation by enacting laws to combat the negative challenges that the introduction of Information Technology and Systems bring?

🏋 Self Assessment 2-6

1 If your mate is easily irritated, impatient, becomes incensed or alarmed when for example his/her PC takes a few seconds longer to perform a task and expect you to provide instant response, then he/she is likely to be suffering from \_\_\_\_\_\_\_\_\_.

1. Repetitive Stress disorder
2. Technostress
3. Computer Vision Syndrome
4. Carpal Tunnel Syndrome

2. Computer-monitoring systems can

I. take snap shots of employees computer monitors

II. record how many breaks an employee is taking

III. track every keystroke made by the user

a. I and II only

b. I and III only

c. II and III only

d. I, II and III

e. II only

3. Which of these is not a form of employee monitoring?

a. Phone calls monitoring

b. Video taping

c. Computer files reviewing

d. Tracking of Internet usage

e. None of the above

4. The most important occupational disease in industrialized countries today is \_\_\_\_\_\_\_\_\_\_.

a. Computer Vision Syndrome

b. Technostress

c. Hepatitis-B

d. Repetitive Stress Injury

e. All of the above

5. The dimension of digital divide that refers to the difference in Internet access between the rich and poor within a particular country is known as \_\_\_\_\_\_\_\_\_\_.

a. Internet divide

b. Social divide

c. Global divide

d. Computer illiteracy

e. All of the above

 *Learning Track Activities*

|  |  |
| --- | --- |
| j0299125 | **Unit Assignments 6**   1. Why do Information Systems executives whose staffs develop systems that cause harm to others face difficulties? 2. Why is it thought that liability laws will extend its reach to include software even when it merely provides an information service? 3. Explain the logic of “automation optimists” who hold the view that automation will rather cause a net increase in jobs, not a decrease. 4. How can IT lead to changes in the structure of an organization? 5. List five advantages and five disadvantages of Teleworking. |

Selected Answers to Self Assessments

**Self assessment 1-1**

**Question Answer**

1 a

2 e

3 b

4 d

**Self assessment 2-1**

**Question Answer**

1 c

2 b

3 e

4 c

**Self assessment 1-2**

**Question Answer**

1 c

2 e

3 d

4 c

5 b

**Self assessment 2-2**

**Question Answer**

1 c

2 a

3 a

4 c

5 c

**Self assessment 1-3**

**Question Answer**

1 c

2 d

3 a

4 b

5 c

**Self assessment 2-3**

**Question Answer**

1 a

2 c

3 b

4 c

5 b

**Self assessment 1-4**

**Question Answer**

1 b

2 a

3 d

4 d

5 b

**Self assessment 2-4**

**Question Answer**

1 e

2 b

3 e

4 c

5 c

**Self assessment 1-5**

**Question Answer**

1 d

2 b

3 e

4 c

5 e

**Self assessment 2-5**

**Question Answer**

1 c

2 c

3 e

4 c

5 e

**Self assessment 1-6**

**Question Answer**

1 d

2 e

3 c

4 e

5 c

**Self assessment 2-6**

**Question Answer**

1 b

2 d

3 e

4 d

5 b

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| = = = = = = = = = = = = = = = == = = = = = = detach and return to IDL, KNUST = = = = = = = = = = = = = = = = = = = = | ***Learner Feedback Form/[insert course code]***  Dear Learner,  While studying the units in the course, you may have found certain portions of the text difficult to comprehend. We wish to know your difficulties and suggestions, in order to improve the course. Therefore, we request you to fill out and send the following questionnaire, which pertains to this course. If you find the space provided insufficient, kindly use a separate sheet.   1. How many hours did you need for studying the units  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | Unit no. | 1 | 2 | 3 | 4 | 5 | 6 | | No. of hours |  |  |  |  |  |  |  1. Please give your reactions to the following items based on your reading of the course  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | **Items** | **Excellent** | **Very good** | **Good** | **Poor** | *Give specific examples, if poor* | | *Presentation quality* | ⬜ | ⬜ | ⬜ | ⬜ |  | | *Language and style* | ⬜ | ⬜ | ⬜ | ⬜ |  | | *Illustrations used (diagrams, tables, etc.)* | ⬜ | ⬜ | ⬜ | ⬜ |  | | *Conceptual clarity* | ⬜ | ⬜ | ⬜ | ⬜ |  | | *Self assessment* | ⬜ | ⬜ | ⬜ | ⬜ |  | | *Feedback to SA* | ⬜ | ⬜ | ⬜ | ⬜ |  |  1. Any other comments |