



Introduction to Computer Ethics

Software Engineering Professional Ethics
Course Teacher: Debabrata Mallick (DM)

Background Of Ethics

- **Ethics: a set of beliefs about right and wrong behavior.**
- According to Socrates (Greek philosopher, 477 - 399 BC): People will naturally do what is good, if they know what is right
- Evil or bad actions (Hacking Cyber Crimes) are the result of unawareness about right and wrong
- so, if a criminal were truly aware of the mental and spiritual consequences of his actions, he would neither commit nor even consider committing them
- therefore, any person who knows what is truly right will automatically do it

Definition

- Ethics: “The science of morals; the department of study concerned with the principles of human duty. The moral principles by which a person is guided.” – Oxford English Dictionary
- Moral: “Of or pertaining to character or disposition, considered as good or bad, virtuous or vicious; of or pertaining to the distinction between right and wrong, or good and evil, in relation to the actions, volitions, or character of responsible beings; ethical.” – Oxford English Dictionary
- Terms will be used interchangeably – basically, knowing the difference between right and wrong.



Introduction

- In the industrialized world computers are changing everything: from education to health, from voting to making friends or making war.
- Developing countries can also fully participate in cyberspace and make use of opportunities offered by global networks.
- We are living a technological and informational revolution.
- It is therefore important for policy makers, leaders, teachers, computer professionals and all social thinkers to get involved in the social and ethical impacts of this communication technology.

Computer Ethics

- The components of an ethical computer system are responsibility, ownership, access and personal privacy.
 - Responsibility concerns the accuracy and accountability of the information (using information properly)
 - Ownership deals with who has the right to use the information (information belongs to)
 - Access deals with who is allowed to use, view, store and process the information. (eligible to use information)
 - Personal privacy addresses the question of who the information belongs to (respect of personal information)

Impact of Cyber-Crime

1. Fraud and **Embezzlement**

- The most significant losses to businesses from computer crime come from employees.
- Losses from credit card fraud are estimated to be between \$1 and \$4 billion per year.
- ATM fraud accounts for losses of about \$60 million a year
- Telecommunications fraud estimated around \$1 to \$9 billion each year.
- Why? *Tradeoff between convenience and security*

2. Sabotage and Information Theft

- Direct destruction of hardware, software or information
- Use of “logic bombs”
- An employee fired from an insurance company was convicted for destroying more than 160,000 records.
- British Airways paid a competitor \$4 million after hacking into their computers and stealing passenger lists.
- Identity Theft (Information Collection, Privacy

3. Hacking and Cracking

- Kevin Mitnick, a notorious hacker, was arrested in 1995. He allegedly stole thousands of files from a computer security expert, credit card numbers, and unreleased software. (Book: *Takedown* by T. Shimomura)
- High-Tech Low-Tech tricks:
- Social Engineering, Shoulder Surfing
- Clifford Stoll's *The Cuckoo's Egg* written about tracking a German hacker.
- In the 1970's John Draper discovered that the whistle in a cereal box could be used to fool the telephone system into giving free long-distance calls.

Cyberethics and cybertechnology

- **Cyber-technology** refers to a broad range of technologies from stand-alone computers to the cluster of networked computing, information and communication technologies.
- **Cyber-ethics** is the field of applied ethics that examines moral, legal, and social issues in the development and use of Cyber-technology.
- Internet ethics and information ethics.

Computer ethics: definition

- Same as cyber-ethics, or
- The study of ethical issues that are associated primarily with computing machines and the computing profession.
- The field of applied professional ethics dealing with ethical problems transformed, or created by computer technology

Computer Ethics:

Some historical milestones

- ❑ 1940-1950: Founded by MIT prof Norbert Wiener: cybernetics-science of information feedback systems.
- ❑ 1960s: Donn Parker from California examined unethical and illegal uses of computers by professionals. 1st code of professional conduct for the ACM.
- ❑ 1970: Joseph Weizenbaum, prof at MIT, created Eliza.
- ❑ Mid 1970: Walter Maner taught 1st course and starter kit in computer ethics

Computer ethics history (cont.)

- 1980: Issues like computer-enabled crime, disasters, invasion of privacy via databases, law suits about software ownership became public.
- Mid 80s: James Moore of Dartmouth, Deborah Johnson of Rensselaer, Sherry Turkle of MIT, and Judith Perrole published article and books.

Computer ethics history (cont.)

- 1990: Interest in computer ethics as a field of research had spread to Europe and Australia.
- Simon Rogerson of De Montfort University (UK) Terrell Bynum, editor of Metaphilosophy (USA), initiated international conferences.
- Mid 90s: Beginning of a 2nd generation of computer ethics with more practical action.
- 2004: Interest spreads to Cotonou, Benin

Any unique moral issues?

Deborah Johnson: Ethics on-line

- The **scope** of the Internet is **global** and **interactive**.
- The Internet enables users to interact with **privacy**.
- Internet technology makes the **reproducibility** of information possible in ways not possible before.
- The above features make behavior on-line morally different than off-line.

The debate continues:

- James Moore: Computer technology is “logically malleable” unlike previous technologies. It can create “new possibilities for human action”.
- Brey: disclosing non-obvious features embedded in computer systems that can have moral implications.
- Alison Adams: Take into account gender-related biases. Combine feminist ethics with empirical studies.

Sample topics in computer ethics

- ❑ Computers in the workplace: a threat to jobs? De-skilling? Health and safety?
- ❑ Computer security: Viruses. Spying by hackers.
- ❑ Logical security:
Privacy, integrity, consistency, controlling access to resources.
- ❑ Software ownership: Intellectual property vs. open source.
- ❑ Software development: quality, safety

Computers in the workplace

- Monitoring of employees: employer vs. employee point of view.
- Loyalty
- Health issues.
- Use of contingent workers.
- A threat to jobs.
- De-skilling.

Computer security

- ❑ Viruses: programming code disguised
- ❑ Worms: propagate w/o human intervention(involvement)
- ❑ Trojan horses: gets secretly installed.
- ❑ Logic bombs: execute conditionally.
- ❑ Bacteria or rabbits: multiply rapidly.
- ❑ Computer crimes: embezzlement(theft, misuse, stealing).
- ❑ Hackers: vandalism or exploration.

Logical security

- Privacy invasion of email, files, and own computer (cookies).
- Shared databases.
- Identity theft.
- Combating terrorism: USA Patriot act.

Software ownership

- Knowledge: private greed, public good.
- Profit vs. affordability
- Freedom of expression and access to information
- Right to communicate: share and learn in a globalized world.
- Digital divide is immoral.
- Open source software: Linux. Open access.
- North-South information flow. Indigenous knowledge.



Codes of ethics

- Avoid harm to others
- Be honest and trustworthy
- Acquire and maintain professional competence
- Know and respect existing laws pertaining to professional work
- No personal interest
- Be honest and realistic in stating claims or estimates based on available data

Cases in 2012

- ❑ Cyber criminals target Skype, Facebook and Windows users
- ❑ Cyber criminals targeted users of Skype, Facebook and Windows using multiple Blackhole exploits in October, according to the latest threat report from security firm GFI Software.
- ❑ Researchers uncovered a large number of Blackhole exploits disguised as Windows licences, Facebook account verification emails, Skype

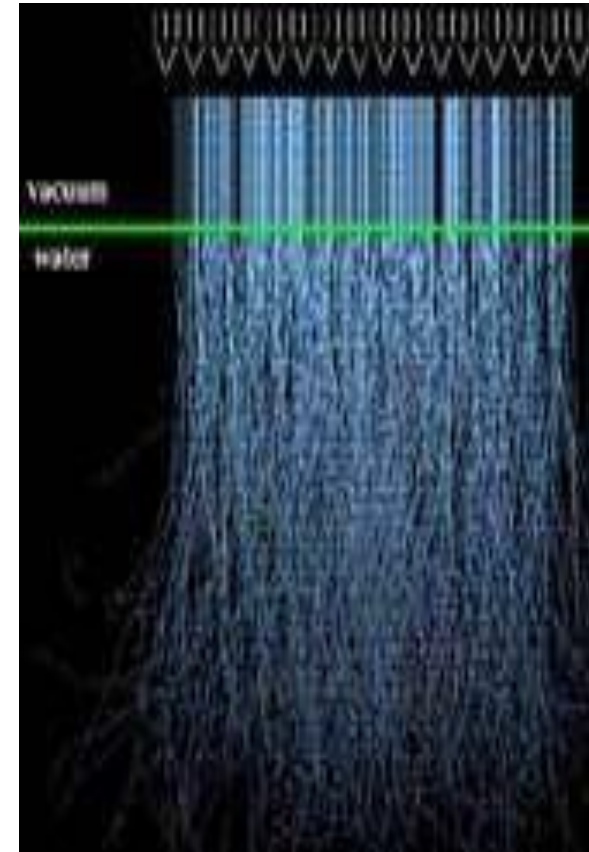


Cases Continues

- Cyber attackers increasingly targeting applications, research shows
- Web and mobile applications are the new frontiers in the war against cyber attack, according to a top cyber security risks report from Hewlett Packard (HP) published in May.
- The report reveals that SQL injection (SQLi) attacks on web applications increased sharply from around 15 million in 2010 to more than 50 million in 2011.

Case Continues

- Therac-25
- Therac-25 was a medical linear accelerator, a device used to treat cancer. What made Therac-25 unique at the time of its use was the software. Not only did the software ease the laborious set-up process, but it also monitored the safety of the machine. In this case on safety critical software, you will find that some patients received much more radiation than prescribed despite the software



Case Continues

- Machado
- At age 19, Richard Machado was the first individual to be convicted of a federal electronic mail (e-mail) hate crime. The Machado case is one example of a handful of similar incidents that have occurred since the advent of the Internet.



Authorities say they caught Machado sending the messages on this surveillance videotape (CNN)

Case Continues

- Hughes Aircraft
- Between 1985 and 1987, the Microelectronic Circuits Division of Hughes Aircraft shipped hybrid microelectronics to every branch of the U.S. military without completing various environmental chip testing processes required by contract. This is a whistleblower case where the allegations against Hughes Aircraft resulted in a criminal case and a civil case.



Cyber-Crime Cases

- For more Cyber cases follow the link below
- <http://www.computerweekly.com/news/2240174301/Top-10-cyber-crime-stories-of-2012>
- <http://abcnews.go.com/US/harvard-ethics-student-charged-hacking-mit-computer/story?id=14110364>

Ten Commandments

- ❑ 1. Not use a computer to harm other people. This is the foundation for computer ethics.



Ten Commandments

- ❑ 2. Not interfere with other people's computer work.
Such as sending numerous thoughtless e-mails to larger issues like purposely sending computer



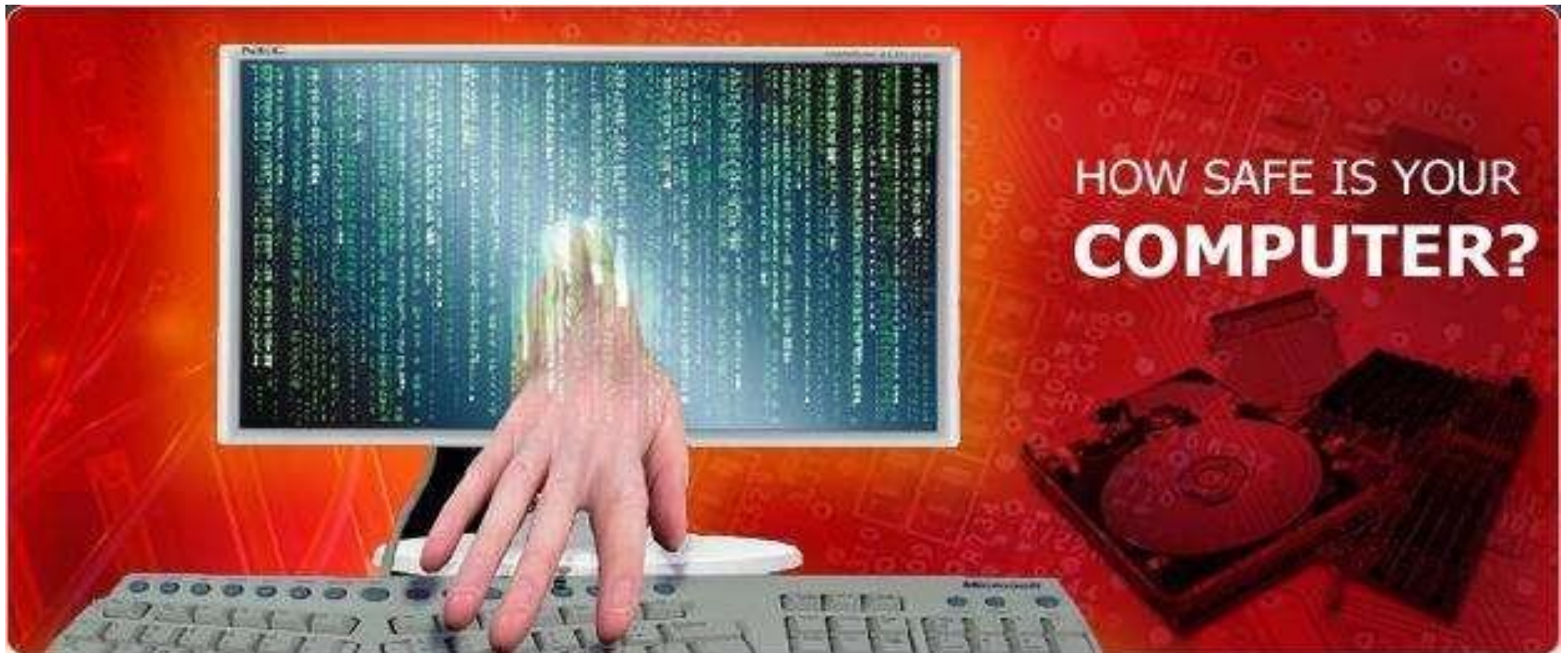
Ten Commandments

- ❑ 3. Not snoop around in other people's computer files. Don't go looking through other people's computer files unless given permission.



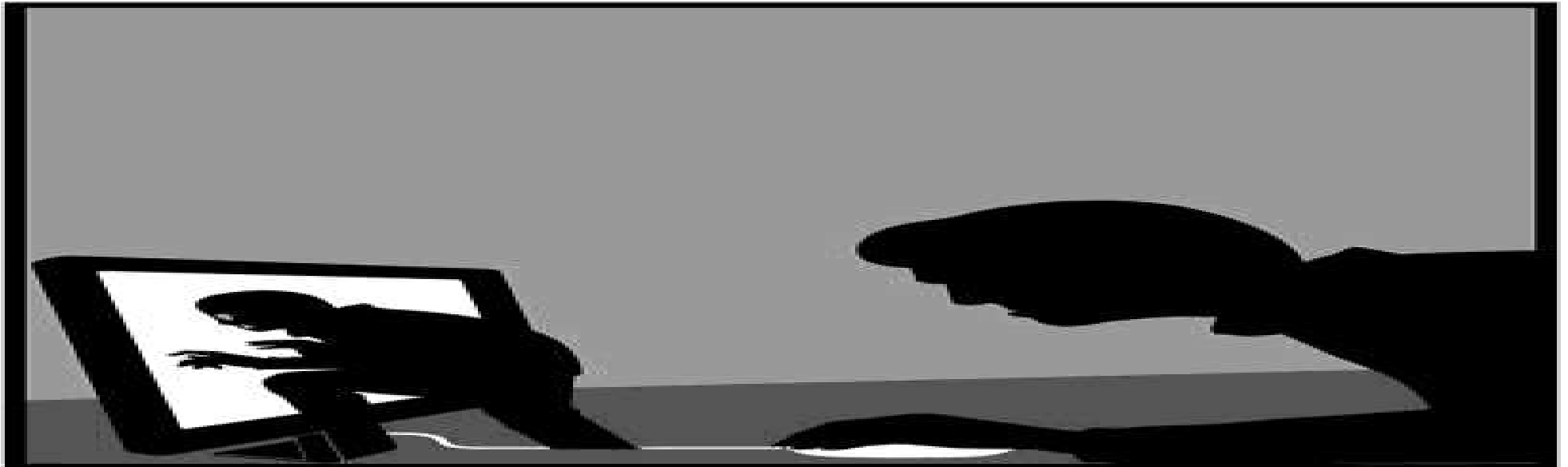
Ten Commandments

- ❑ 4. Not use a computer to steal.



Ten Commandments

- ❑ 5. Not use a computer to bear false witness. Don't spread rumors or change your email address so that the receiver of an email believes that it came from someone other than yourself.



Ten Commandments

- ❑ 6. Not copy or use proprietary software for which you have not paid. Once you buy a software system, music CD or DVD you should not make copies of that information and distribute it to your friends.



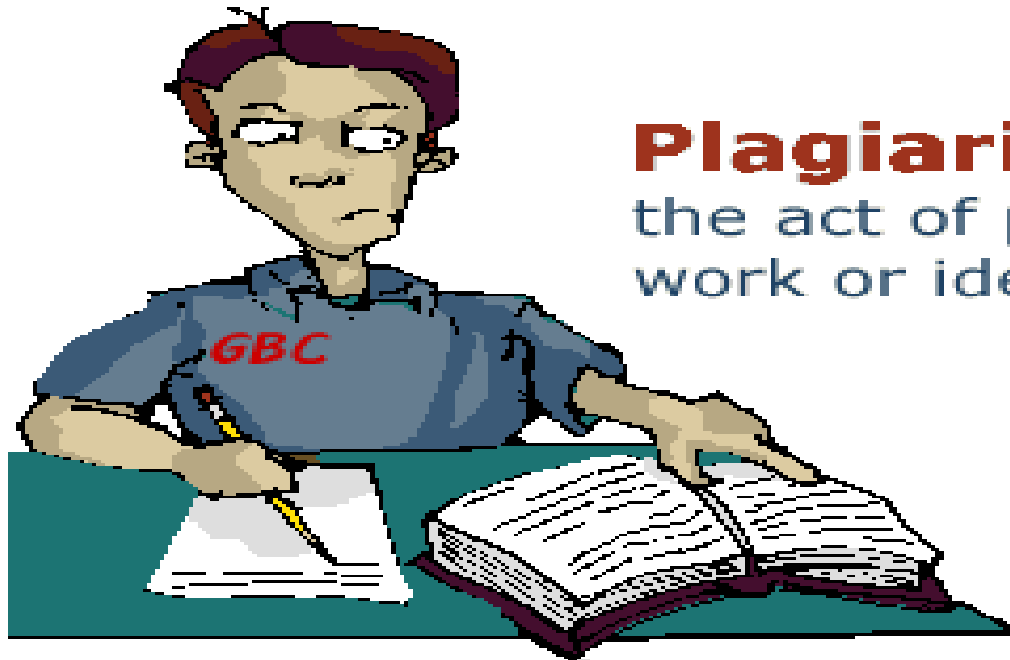
Ten Commandments

- ❑ 7. Not use other people's computer resources without authorization or proper compensation. This means do not surf the internet or print off large amounts of paper for personal use during work hours.



Ten Commandments

- ❑ 8. Not appropriate other people's intellectual output. Don't upload information and take credit for it such as music, images and text.



Plagiarism:

the act of presenting another's work or ideas as your own.

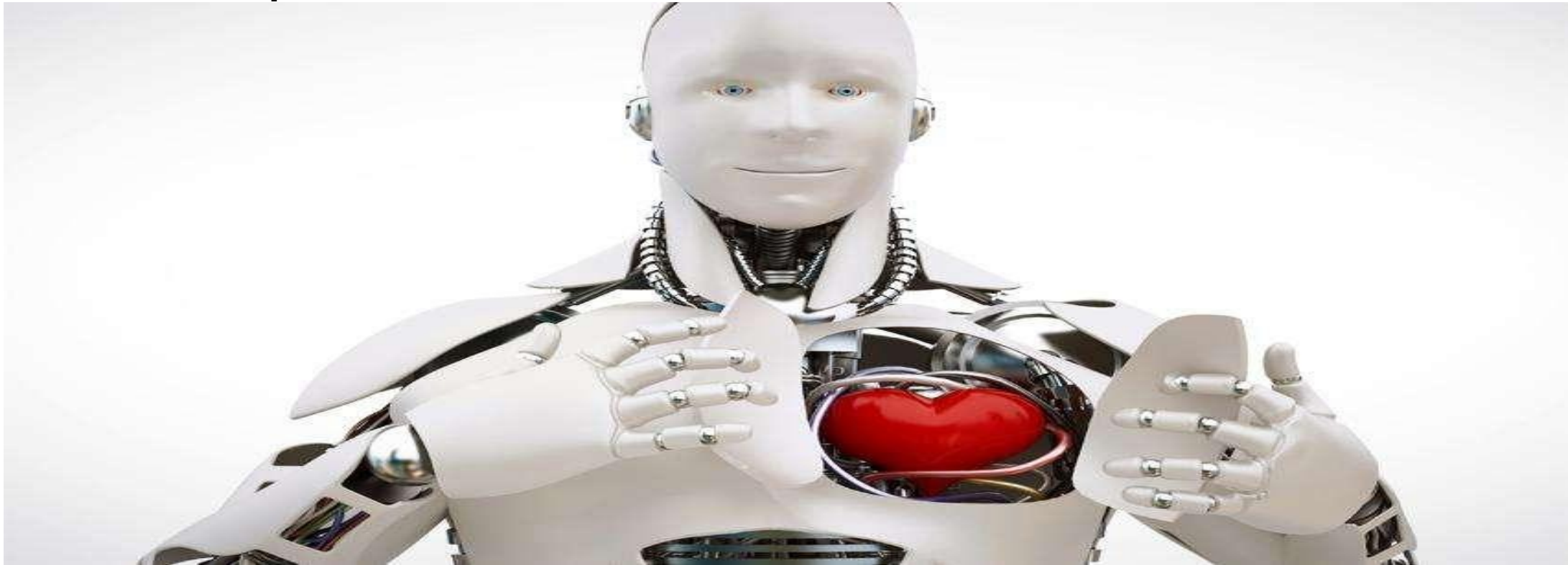
Ten Commandments

- 9. Think about the social consequences of the program you are writing or the system you are designing.



Ten Commandments

- ❑ 10. Use a computer in ways that ensure consideration and respect for your fellow humans. Just because you can't always see someone face to face doesn't give you the right to offer any less respect than you would offer in a personal encounter.





Ten Commandments of Computer Ethics:

- 1. You shall not use a computer to harm other people**
- 2. You shall not interfere with other people's computer work**
- 3- You shall not snoop around in other people's computer files**
- 4. You shall not use a computer to steal**
- 5 You shall not use a computer to bear false witness**
- 6 You shall not copy or use proprietary software for which you have not paid**
- 7. You shall not use other people's computer resources without authorization or proper compensation**
- 8. You shall not appropriate other people's intellectual output**
- 9. You shall think about the social consequences of the program you are writing or the system you are designing**
- 10. You shall always use a computer in ways that show consideration and respect for your fellow humans.**

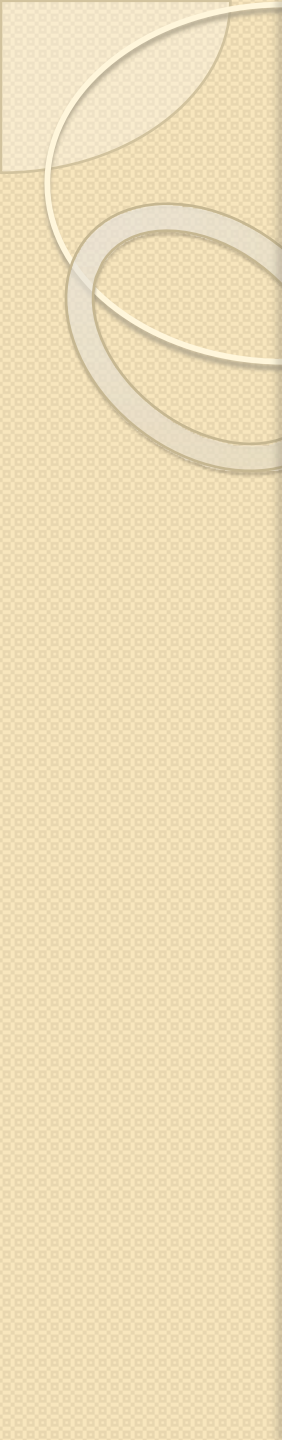


Codes of Ethics for Computer Professionals:

1. Central concern: the public good, including human rights and diversity of culture-
2. Honesty and fairness in communication about software and related topics
3. Use client or employer property only as authorized
4. High quality, reasonable cost and schedule
5. Respect for privacy, intellectual property
6. Disclose conflicts of interest
7. Address software errors
8. Lifelong learning
9. Honor agreements and assigned responsibilities

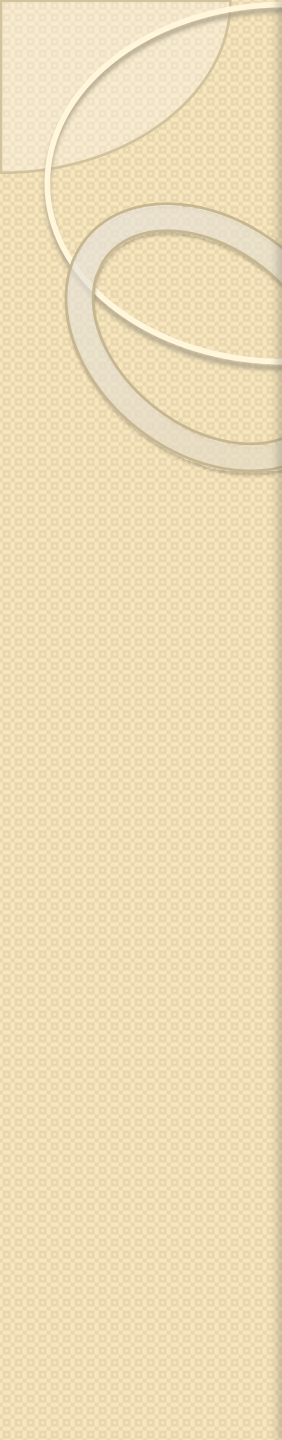
Scenario 1 – *Illegal Use*

- A person is using a piece of SW without the author's permission and says: "I'm not really using it, I'm just evaluating it before I make a firm decision on buying"
- That person is "evaluating" that piece of SW for 12 months now!
- **Is the conduct of that person ethical?**



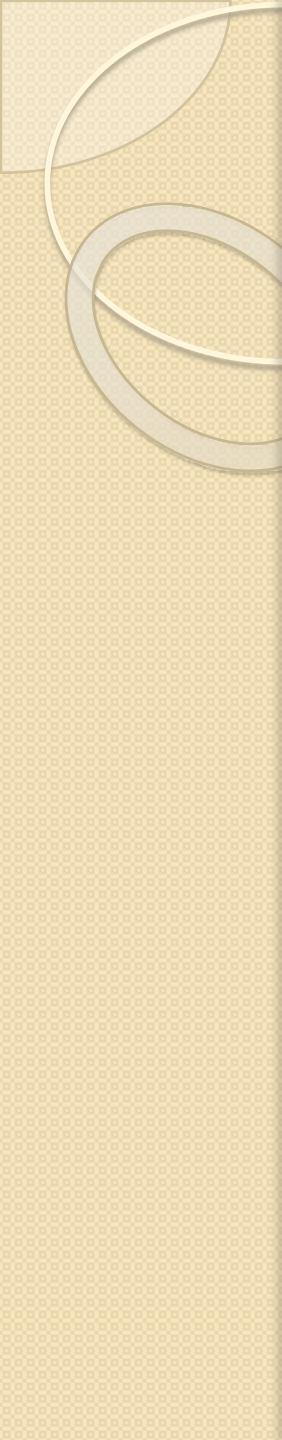
■ Scenario 2 – *Vaporware*

- A small company announces a new SW product
- A larger, more established competitor hears about that product, and starts a whispering campaign that she is also working on a similar product that will be released soon.
- Potential customers decide to wait for the product instead of making the more riskier purchase from the smaller company.
- The new company's sales become sluggish, and it fails to earn back the investment that it has put into developing that new product. That results in her closure.
- The larger company never releases the promised product.
- **Is the conduct of that large company unethical or a reasonable business tactic?**



■ Scenario 3 – *Whistle Blower*

- SW bugs, at times, have catastrophic consequences
- While A was working for a contractor at NASA, he found such a bug and reported it to his boss, B, who ordered him to never mention it to any one, or he will get fired
- A got scared, and did as he was told
- **Did A behave in an ethical manner? Would you hire him in your company?**
 - Truth (Disclosure) vs. Loyalty (Confidentiality)



■ **Scenario 4 – *Trade Secrets***

- A was working at XYZSoft
- He leaves it to work for a competitor, SuperSoft
- Even before starting at SuperSoft, he already has revealed many of the trade secrets of XYZSoft during his interviews at SuperSoft, giving them an advantage over XYZSoft
- **Do you agree with A's ethics? Would you hire him in your company?**



■ Scenario 5

- You are asked to develop software that stores and manages customers financial data.
- You find a security flaw days before its delivery to the client.
- Your boss tells you to sit on it and will be fixed with a patch after the delivery.
- If you bring the flaw to the foreground it will delay the release and cost your company millions.
- **What do you do?**



■ Scenario 6

- You work for a small software firm that is contracted to write a program that can predict the spread of radiation of a dirty bomb with 75% accuracy.
- The best you have been able to achieve is 74.6% accuracy.
- Your boss says close enough and rounds up the test data.
- **What will you do?**

CASE STUDY

- <http://www.mit.edu/activities/safe/safe/cases/umich-baker-story/Baker/timeline.html>
- <http://www.mit.edu/activities/safe/safe/cases/umich-baker-story/throwout.1>

International Papers Links

- <http://www.ijie.org>, International Journal of Information Ethics.
- www.sans.org/topten.htm Top ten Internet security flaws that system administrators must eliminate to avoid becoming an easy target.
- <http://ethics.csc.ncsu.edu/> Computer ethics as a map.
- <http://www.neiu.edu/~ncaftori/ethics-course.htm>
- The ethics course I borrowed these overheads from.