



Ethics & Professional Responsibility for CS & SE

Summer 2012 REU
Dr. Janell Straach


Trivia:

- What did the Greek God Prometheus (according to Greek Mythology) give as a gift to man?
- A couple of FYIs
 - Zeus was NOT happy!!!
 - Hermes (another Greek God) was credited with discovering how to produce it



What are the benefits of Fire?






What are the negative consequences of Fire?



Is fire Good or Evil?





Trivia #2: What do the following have in common???

- Brooklyn Bridge
- Panama Canal
- Great pyramids
- Statue of Liberty
- Roman aquaducts



Were there ethical dilemmas?

Was professional responsibility
required?



Rapid Pace of Technology Change

- 1940s: The first computer is built
- 1956: First hard-disk drive weighed a ton and stored five megabytes
- 2006: Pocket devices hold a terabyte (one trillion bytes) of data
- 1991: Space shuttle had a one-megahertz computer
- 2006: Automobiles can have 100-megahertz computers
- 2011: iPhone 4s has a 1 GHz processor

Is technology Good or Evil?





Ethics

What is Ethics:

- Study of what it means to “do the right thing”
- Assumes people are rational and make free choices
- Rules to follow in our interactions and our actions that affect others



Question

- Is it ever okay to lie?

Important Ethics Distinctions

- Right, Wrong, and Okay
 - Can't always divide into only two categories
- Difference between wrong and harm
 - Ethical acts can cause other harm – e.g. you take a job which means someone else doesn't
- Separate goal from actions
 - Goal is to make a profit which is ethical
- Personal preference and ethics
- Law and Ethics
 - New law lags behind technology



Characteristics of a Profession

- Initial professional education
- Accreditation
- Skills development
- Certification
- Licensing
- Professional development
- Code of ethics
- Professional society

Software Engineers

- Certification and licensing not needed
- Without these, other characteristics are irrelevant
 - No college education needed
 - No apprenticeship needed
 - No membership in professional society needed
 - No continuing education needed
- Most software engineers are part of teams
- Software engineers have ability to harm public

Professional Codes of Ethics

- A professional code of ethics states the principles and core values that are essential to the work of a particular occupational group
- Main parts:
 - Outlines what the professional organization aspires to become
 - Lists rules and principles by which members of the organization are expected to abide

Where to get Ethics Guidance?





Three Suggested Sources for Code of Ethics

- ACM
- IEEE
- NSPE

ACM Code of Ethics (1)

- General moral imperatives: “As an ACM member I will...”
 1. Contribute to society and human well-being.
 2. Avoid harm to others.
 3. Be honest and trustworthy.
 4. Be fair and take action not to discriminate.
 5. honor property rights including copyrights and patents.
 6. Give proper credit for intellectual property.
 7. Respect the privacy of others.
 8. honor confidentiality.

ACM Code of Ethics (2)

- Specific professional responsibilities: “As an ACM computing professional I will”:
 1. Strive to achieve the highest quality, effectiveness and dignity in both the process and products of professional work.
 2. Acquire and maintain professional competence.
 3. Know and respect existing laws pertaining to professional work.
 4. Accept and provide appropriate professional review.
 5. Give comprehensive and thorough evaluations of computer system and their impacts, including analysis of possible risks.
 6. honor contracts, agreements, and assigned responsibilities.
 7. Improve public understanding of computing and its consequences.
 8. Access computing and communication resources only when authorized to do so.

ACM Code of Ethics (3)

- Organization leadership imperatives: “As an ACM member and an organizational leader, I will:”
 1. Articulate social responsibilities of members of an organizational unit and encourage full acceptance of those responsibilities.
 2. Manage personnel and resources to design and build information systems that enhance the quality of working life.
 3. Acknowledge and support proper and authorized uses of an organization’s computing and communication resources.
 4. Ensure that users and those who will be affected by a design have their needs clearly articulated during the assessment and design of requirements; later the system must be validated to meet requirements.
 5. Articulate and support policies that protect the dignity of users and others affected by a computing system.
 6. Create opportunities for members of the organization to learn the principles and limitations of computer systems.

ACM Code of Ethics (4)

- Compliance with the Code: “As an ACM member, I will:”
 1. Uphold and promote the principles of this Code.
 2. Treat violations of this code as inconsistent with membership in the ACM.

SE Code of Ethics 5.2

- Software engineers shall commit themselves to making the analysis, specification, design, development, testing and maintenance of software a beneficial and respected profession. In accordance with their commitment to the health, safety and welfare of the public, software engineers shall adhere to the following Eight Principles:
- 1 PUBLIC - Software engineers shall act consistently with the public interest.
- 2 CLIENT AND EMPLOYER - Software engineers shall act in a manner that is in the best interests of their client and employer, consistent with the public interest.
- 3 PRODUCT - Software engineers shall ensure that their products and related modifications meet the highest professional standards possible.
- 4 JUDGMENT - Software engineers shall maintain integrity and independence in their professional judgment.
- 5 MANAGEMENT - Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance.
- 6 PROFESSION - Software engineers shall advance the integrity and reputation of the profession consistent with the public interest.
- 7 COLLEAGUES - Software engineers shall be fair to and supportive of their colleagues.
- 8 SELF - Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession.

National Society of Professional Engineers Code of Ethics

- Engineers, in the fulfillment of their professional duties, shall:
 - Hold paramount the safety, health, and welfare of the public.
 - Perform services only in areas of their competence.
 - Issue public statements only in an objective and truthful manner.
 - Act for each employer or client as faithful agents or trustees.
 - Avoid deceptive acts.
 - Conduct themselves honorably, responsibly, ethically, and lawfully so as to enhance the honor, reputation, and usefulness of the profession.

Case Studies...

- ... to get you thinking about ethics!
- Real case studies
- Names have been changed
- Fictional names used ;-)

Ethical decision making

- Three years ago, Tiffany started her own consulting business
 - She is so successful she now has several people working for her.
 - Has many clients.
 - Includes work such as advising on network architectures, designing DBMSes, security.
- Presently designing a DBMS for the personnel office of a medium-sized (100 person) company.
 - Tiffany has involved client in design process
 - Informs CEO, CTO and human resources head about system progress

Ethical decision making

- Now it is time to make decisions about the kind and degree of security to build into system.
- Tiffany has described several options.
- Because of cost overruns, client has decided to opt for a less secure system.
 - Tiffany believes information they will store is extremely sensitive (performance evaluations, medical records for insurance claims, salaries, etc.)
- With weak security:
 - Employees on workstations could figure out how to access this data.
 - Online intruders would also have access

Ethical decision making

- Tiffany feels strongly that system should be much more secure.
 - She has tried to explain the risk.
 - CEO, CTO and HR all agree that less security will do.
- What should Tiffany do?
 - Should she refuse to build the system as they request?

Applying the Code

- This case highlights issues involving privacy
 - Principle 1.7 deals with privacy
 - Principle 1.8 deals with confidentiality
- Code guidelines state that:
 - “computer professionals are obligated to preserve the integrity of data about individuals...”
 - “... from unauthorized access or accidental disclosure to inappropriate individuals”
- Code also specifies for organizational leaders:
 - Principle 3.5 (enhance personal dignity)
 - Principle 3.4 (assess needs of all those affected by system)

Applying the Code

- Company officials:
 - Have an obligation to protect privacy of their employees.
 - Therefore they should not accept inadequate security.
- Tiffany's first obligation:
 - Attempt to educate company officials (implied by principle 2.7)
- If that fails, she needs to consider her contractual obligations (principle 2.6) in honoring assigned responsibilities.
- We don't have Tiffany's contract, but she may have to choose between her contract and her obligation to honor privacy and security.

Ethical Decision Making

- Aisha works in a large provincial agency dealing with alcoholism and drug abuse.
- Agency administers programs for individuals with alcohol and drug programs.
 - Maintains a large database of information on clients who use agency services.
 - Some data files contain names and current addresses of clients.
- Aisha has been asked to look at the track records of treatment programs.
 - Reporting # of clients seen each month for past five years, length of client treatment, number of clients who return after program completion, criminal histories of clients.

Ethical Decision Making

- Aisha has been given access to all files in the agency's mainframe computer
 - This data is needed to put together the report.
- After assembling data:
 - She downloads it to the computer in her office.
- The agency is pressuring her to finish report on the deadline.
 - Aisha decides she must work from home over the weekend.
 - She copies data onto a USB drive and takes it home.
 - After finishing the report she leaves the USB drive at home and forgets about it.

Applying the Code

- This case resembles previous case, but raises several additional issues.
- Issues involving confidentiality
 - Principle 1.7 deals with privacy
 - Principle 1.8 deals with confidentiality
- Principle 2.8 also applies:
 - Constraining access to authorized systems
- Principle 3.5:
 - Organizational leaders have obligations to “verify systems are designed and implemented to protect personal privacy and enhance personal dignity”
- Also Principle 3.3:
 - (Appropriate and authorized uses of organization’s resources)

Applying the Code

- Government agency should have had policies and procedures to protect identity of its clients
 - Aisha's friends and relatives might accidentally discover files and inappropriate uses information.
 - Note that the files Aisha used did not need to have names or other information in the records.
- Agency should have removed identifying information from files Aisha was allowed to use.
 - If this happened, it wouldn't have mattered that Aisha copied files to her computer.
- Aisha, unfortunately, was not attentive to ethical issues ahead of time.

Ethical decision making

- Zach is a database programmer
 - large statistical program needed by his company (actuarial requirements)
 - company programmers are encouraged to publicize their work
- Zach has found himself stuck on a problem
 - Has persisted at this for several months.
 - His manager does not recognize complexity of problem.
 - She insists job be completed in the few days.
- Zach remembers:
 - co-worker had given him source listings of their current work
 - he also has an early version of commercial software developed at another company

Ethical decision making

- Zach studies these programs
 - Sees two areas of code which could be directly incorporated into his own program
 - He uses segments of code both from his coworker and from the commercial software
 - He does not tell anyone or mention it in the documentation.
- He completes the project and turns it in a day ahead of time.
- How does the Code of Ethics help us understand this case?

Applying the code

- This case highlights issues involving intellectual property
 - 1.6: “Give proper credit for intellectual property”
 - Specifically, do not take credit for other’s ideas or work.
- Property rights principle (1.5)
 - copyrights, patents, trade secrets, license agreements
- Restrictions also ground in:
 - integrity (1.3)
 - complying with existing laws (2.3)

Applying the code

- Zach violated professional ethics in two areas:
 - Failure to give credit for another's work.
 - Using code from a commercial package that (presumably) was copyrighted.
- If Zach only “looked” at co-worker's source code:
 - Could he then write his own program and still have an obligation to give credit?
- Yes:
 - He should have acknowledged credit in documentation.
 - (Some professional discretion possible here, especially if intellectual material is trivial.)

Applying the code

- Use of commercial software code was also not appropriate:
 - Zach should have checked to determine whether or not company was authorized to use source code before using it.
- In general:
 - Desirable to share and exchange intellectual materials
 - But using bootlegged software is definitely a violation of code.

NSPE Case Study -- SPQ

- Alfonso is employed by SPQ Engineering, an engineering firm in private practice involved in the design of bridges and other structures. As part of its services, SPQ Engineering uses a CAD software design product under a licensing agreement with a vendor. Under the terms of the licensing agreement, SPQ Engineering is not permitted to use the software at more than one workstation without paying a higher licensing fee.
- SPQ Engineering ignores this restriction and uses the software at a number of employee workstations. Alfonso becomes aware of this practice and calls a “hotline” publicized in a technical publication and reports his employer’s activities.



NSPE Case Study

- **Question:**
- Was it ethical for Alfonso to report his employer's apparent violation of the licensing agreement on the "hotline" without first discussing his concerns with his employer?

NSPE response

- It was determined that it was not ethical for Alfonso to report his employer's apparent violation of the licensing agreement on the "hotline" without first discussing his concerns with his employer.
- The facts and circumstances were not of a character that involve any danger -- direct or indirect -- to the public health and safety. Instead, the facts and circumstances related to matters of a legal nature and do not relate to engineering judgment or expertise.

NSPE response

- The Board noted that NSPE Code Section II.4. places a basic obligation on engineers to be faithful agents and trustees in professional matters with their employers. The Board also noted that it was troubled that Alfonso did not consider other less adversarial and surreptitious alternatives. For example, Alfonso could have first discussed this matter with his employer, pointing out the possible damages that the violation posed to SPQ Engineering, and suggesting that SPQ Engineering confer with its legal counsel before continuing its current actions. Instead, Alfonso took a course of action that could cause significant damage to SPQ Engineering and ultimately to Alfonso himself.

NSPE response

- The Board was inclined to wonder about the motivation for Alfonso's actions without his first exploring other less adversarial and surreptitious alternatives -- in view of the lack of any direct danger to the public health and safety. While, in the context of the facts of this case, the Board could not conclude that this provision compels Alfonso to ignore an apparent violation of the law and the NSPE Code (See NSPE Code Section III.9.), the Board concluded that Alfonso could have easily exercised far greater judgment and professional discretion before taking action. Therefore, it was the Board's opinion that A's action in reporting his employer's apparent violation, without first pursuing alternative actions open to him, was in conflict with the Code of Ethics.

NSPE response

- Alfonso has an obligation to pursue this matter with SPQ Engineering. If a satisfactory ethical resolution cannot be reached, he is obligated to report the violation to the vendor. In addition, he should reconsider (under Code Section II.1.d.) his further association with a firm which has shown itself engaged in fraudulent and dishonest enterprise.

NSPE Case Study -- Hospital

- Tej, a young professional engineer with expertise in software engineering, works for a hospital information technology department. He is assigned to work with the people in the intensive care unit (ICU). A computer user group, headed by the lead physician in the ICU, is forced to facilitate interface between a piece of commercial data processing software and various units in the ICU, including real-time patient monitoring devices.

NSPE Case Study -- Hospital

- From the manager on down, the computer user group is not technically up to the mark in experience or in education. The computer user group was falling significantly behind schedule. Tej learns that the group is seriously considering cutting back on testing in order to close the schedule gap. Appalled at this idea, Tej argues strongly against it with the corporate user group. In this case, Tej's arguments has some effect, but Tej is nevertheless given the clear impression that his long-term employment prospects with this organization are now significantly impaired. Apparently, part of the problem had to do with a reluctance on the part of hospital administration to clash with the physician who heads the computer user group. Tej feels that the basic problem is incompetence of the computer user group and he does not see how he could be effective on his own in combating it.



NSPE Case Study -- Hospital

- **Question:**
- What are Tej's obligations under the circumstances?

NSPE Response

- The obligation of engineers to report observations to higher authorities has been a critical issue considered by the Board on earlier occasions. The conflict between an engineer's obligation to loyally serve an employer or client must be balanced with the duty of the engineer to protect the public health, safety, and welfare.
- The Board noted that the facts presented in this case raised a conflict between two basic ethical obligations of an engineer: The obligation of the engineer to be faithful to the client and not to disclose confidential information concerning the business affairs of a client without that client's consent, and the obligation of the engineer to hold paramount the public health and safety.

NSPE response

- Turning to the facts in the present case, the Board believes that the facts establish a sufficient basis for Tej to continue his efforts to attempt to educate higher management about the risks associated with not correcting the engineering and management issues. While Tej is an employee and as such owes some duty of loyalty and duty of confidentiality to the employer, that duty does not extend to situations in which the public health and safety is being compromised and put at significant risk.

NSPE response

- Tej's failure to press ahead with his concerns could place the ICU patients at grave risk and also put the hospital, its board of directors, and employees at risk of liability. Depending upon the facts and circumstances, Tej may be required to exhaust all appropriate and available internal mechanisms and procedures to get hospital administration to focus on this critical issue. If unsuccessful, Tej may be required to take steps to report the issues to an appropriate authority as necessary.

NSPE response

- Tej has an ethical responsibility to attempt to educate the computer user group on the risks and consequences of inadequate testing of the system. If he is not successful, he should continue to make his case to hospital administration. If that fails, he should exhaust all appropriate and available internal mechanisms and procedures up to the body responsible for hospital administration. If Tej is still unsuccessful, they may be required to take steps to report the issue to an appropriate authority as necessary.

Scenario—Michael

- Michael is an average fellow. Like many consumers, he likes to rent a video occasionally, play basketball on Saturday, and visit the park on Sunday. Michael also happens to be a software engineer for a small software development company. Lately, Michael has developed an interest in network programming. His background is mostly in database and user interface programming, and he wanted to learn more.

Scenario—Michael

- So, Michael bought a highly recommended book about network programming and started reading in his free time. One of the examples in the book showed a step-by-step method for building a packet sniffer that would enable him to see his network traffic. Michael, excited at the new project, started following the example and implementing it as he went. He completed the example and was pleased with himself because of the few problems he encountered during the exercise. Then, being the curious type, Michael left the packet sniffer running on a spare computer hooked into his home network to see what data the program would collect. Michael soon forgot about his packet sniffer's running in the background.

Scenario—Michael


- Later that evening, Michael was completing an online purchase facilitated by his digital wallet. He then logged onto some Internet games for recreational distraction. The next morning, Michael sat down at his spare computer and remembered that he had left the packet sniffer running. He browsed through the recorded data and was surprised when he noticed the logs of his online transaction for the portable data storage device. The digital wallet server had sent an unencrypted command to his digital wallet telling it to transmit its important customer information back to the server. With his curiosity piqued, Michael wrote a program that would simulate a digital wallet server and send that command to his digital wallet. To his dismay, the digital wallet transmitted the information without verifying the source of the command.

Scenario—Michael

- Michael collected some more data and contacted the company that created his digital wallet software with his findings. After Michael voiced his concerns to a representative of the company, he was told, “We are aware of that capability, but it is minor and not worth addressing.” Michael was understandably upset. What the company considered minor could cost their users unimaginable amounts of money. The representative assured him that such an occurrence was highly unlikely. Flabbergasted, Michael hung up the phone and was unsure what to do.

Scenario—Analysis (SE Cof E)

- Michael tried to think about the issue in an organized way. First, he considered whom this might affect. He identified four basic stakeholders in the issue: Michael himself, the company, the users of the digital wallet, and the general public. Michael is also one of the users. The most vulnerable of the stakeholders are the users, who are not aware of how vulnerable they are. Michael has an entire range of possible actions, from ignoring the situation to complete public disclosure of the bug. We will consider the following four alternatives within this range:



Scenario—Analysis

- Stay quiet and hope no one finds the problem,
- Inform an appropriate business agency of the problem,
- Go public without revealing the exact details of the problem, and
- Go public and reveal the exact details of the problem.

Scenario—Analysis

- The first alternative is, in a sense, the status quo: do nothing more. If Michael hadn't been snooping around in the first place, there would be no issue. Michael recalls that a friend had told him of some ethical guidelines that could be helpful in weighing the alternatives. So he checked online and found the Software Engineering Code of Ethics. Principles 1.02 and 1.05 call for weighing “the interests of the company with the public good” and cooperation “in efforts to address matters of grave public concern”, and Michael has already notified the company privately of the problem and its consequences. By not going public, he would be protecting the company, and also protecting the public by not disclosing the flaw, unless someone else discovers the bug and violates the privacy of the users.
- Perhaps the company will change its mind and address the bug?

Scenario—Analysis

- The problem with this alternative is that Michael has been told that the company is not interested in fixing the situation, and users' privacy and economic safety are still at risk. These issues are just too important to be ignored. This means the company should be viewed as violators of the code of ethics, and according to principle 6.13, significant violations of the code should be reported to the appropriate authorities. Thus, the alternative of remaining quiet has to be rejected, and Michael feels he must become a whistle-blower, but at what risk.

Scenario—Analysis

- The second alternative Michael could take is to inform appropriate business agencies, such as the Better Business Bureau. By informing these agencies he is trying to follow the Software Engineering Code of Ethics. Imperative 1.04 states that one should tell the appropriate people of any potential danger of software. He had found a problem in the digital wallet and informed the company. Since the company did not respond, another step is needed. By going to the business agencies he would be trying to help every party involved in the situation. By not going public with the issue, he did not expose the vulnerability of the system to everyone. He also helped the company by not exerting public pressure to fix the bug. He identified and defined the problem and then told the business agencies about the bug so they could investigate. By doing this, the business agencies could now be aware of the potential problem in other related products. This again helps the public by creating stricter standards on new software. By informing the business agencies about the problem, Michael still retains his option to go to the public in case the business agencies do not do anything about the problem. This option seems like a good compromise, but is it the best alternative? Michael continued considering the other possibilities.

Scenario—Analysis

- A third alternative is for Michael to go public with the fact that a problem exists without revealing the details of the problem to the public. Following this course, the exact vulnerabilities of the system are not made public (and easily exploitable) while at the same time alerting the users that the software they use is not totally secure. The users could then judiciously restrict their use of the software. The public could also now put pressure on the company to fix the problem. However, because of Michael's reticence to reveal exact details of the problem, the public might not take his alert seriously, and he could be accused of having ulterior motives. Also, even though the exact details would not be released, the vulnerabilities of the system will be known to exist, and inevitably some hackers are going to try to crack the system. Finally, after all is finished, the company still might not fix the problem, dismissing Michael's claims again.

Scenario—Analysis

- A fourth alternative is for Michael to go public and completely reveal the details of the problem. With this information, hackers will be able to commandeer the digital wallet system, which will force the company to fix the problem or lose their entire customer base. If the company fails to respond quickly, however, users could lose large amounts of money and have their privacy violated. If users were aware of the problem they could stop using the digital wallet software, although this would cause some merchants still to lose money. Finally, as a personal effect, Michael's reputation as a software engineer could be damaged as some professionals might see his actions as too extreme. While Michael seems to be upholding points 1.04 and 6.13 as mentioned above, he could be doing more harm than good for the users by revealing all the details.

Scenario—Analysis

- After weighing the pros and cons of these four alternatives, we think that Michael should choose the second alternative and notify an appropriate business agency. The problem is too important just to walk away, and going to the public at this point opens up new problems. By choosing this action, Michael will bring the leverage of the agency to bear on the company while insulating himself from any repercussions associated with the act of whistle blowing. It will also put the users in the least danger in terms of financial and privacy loss. If nothing happens through the agency, Michael still retains the option to go public. That threat may be useful in pressuring the company to fix the bug.

Scenario—Analysis

- Whistle blowing is a tricky endeavor. Usually, the whistle blower has good intentions, but sometimes more harm than good can come from the act. In this paper, we portrayed the case of a software engineer faced with such a decision. Either his action or inaction could cause significant financial damages to the users (including businesses) of a software package. In trying to determine a best course of action, we analyzed four alternatives spaced along the spectrum of action to inaction. While no one general solution exists for all cases of whistle blowing, in our specific case, the solution that was a compromise between both extremes and that isolated both the public and the individual from the consequences of whistle blowing seemed to be the best course.

Ethical decision making

- Computer company is writing first part of an “efficient accounting system”.
 - Will be used by government.
 - Expectation is that this will save taxpayers a considerable amount of money each year.
- Software engineer in charge of design assigns different parts of system to his staff.
 - Reports, Internal Processing, User interface
- Manager is shown the system, and agrees it matches requirements.
- System is installed, but staff find the interface so difficult to use that their complaints are heard by upper-level management



Ethical Decision Making

- Result of complaints:
 - upper-level management will not invest any more money in developing the new accounting system
 - they go back to their original, more expensive system

Applying the ACM Code

- This case highlights issues involving quality of professional work
- Code of Ethics advocates that:
 - professional strive to achieve the highest quality in both process and products (2.1)
- Principle 3.4: users and those affected by a system must have their needs clearly articulated
- Assumption in this case:
 - Failure to deliver a quality product is directly attributable to failure to follow a quality process.
 - Most likely the problems with interface could have been discovered in review process – peers or users (2.4)
- When harm results (in this case with taxpayers), failure to implement quality process clearly violates ethical behavior.

Ethical decision making

- Contractor is determining requirements for an employment agency.
 - Client describes what is needed when displaying applications whose qualifications appear to match those for a particular job.
 - Client also further states that names of white applicants are to be displayed ahead of nonwhites.
 - Further states that names of male applicants are to be displayed ahead of female applicants.
- Recall: ethical code asserts an ACM member will be “fair and take action not to discriminate”

Applying the ACM Code

- This case highlights issues involving fairness and discrimination
- In this case, system designer is asked to build a system that, it appears
 - will be used to favour white males and
 - discriminate against non-whites and females
- From this it would appear that:
 - system designer should not do what he or she is told, plus
 - should also point out the problematic nature of what is being requested and ask client why this is being done
- Making the inquiry is consistent with 2.3, 2.5 and 4.1.

Applying the ACM Code

- If client answers that they plan to use information to favour white males, then:
 - Computer professional should refuse to build the system as proposed.
- To go ahead and build the system would violate:
 - 1.4 (fairness)
 - 2.3 (respecting existing laws)
- It would also be inconsistent with:
 - 1.1 (well-being)
 - 1.2 (avoiding harm)

Ethical decision making

- A software development company has just produced a new software package.
 - It incorporates new tax laws and prepares both individual and small business tax returns
- The president of the company knows that the program has a number of bugs
 - He also believes the first firm to put this kind of software on the market is likely to capture the largest market share.
- The company widely advertises the package.
 - When the product is shipped, it includes a disclaimer of responsibility for errors resulting from the use of the program.

Ethical decision making

- The company expects it will receive a number of complaints, queries, and suggestions for modification.
- The company plans to use these to make changes and eventually issue updated, improved and debugged versions.
- The president argues that this is general industry policy:
 - “Anyone who buys version 1.0 of a program knows this and will take proper precautions.”
- Because of bugs, a number of users filed incorrect tax returns and were penalized by Rev Canada.

Applying the ACM Code

- This case highlights issues involving legal liability for unreliable code
- Software company (and president in particular) violated several principles in the ACM code of ethics
- Since he was aware of bugs in the product, he did not strive to achieve the highest quality (Principle 2.1)
- By failing to inform consumers about bugs to system, principle 2.5 was violated.
- Here the risks to users is so great they have to pay penalties for mistakes which result from the program.
 - By law companies can make disclaimers only when they are in “good conscience” (Disclaimer does not meet legal test, violated principle 2.3)
- President also violates Principle 3.1

Ethical decision making

- Small software company is working on an integrated inventory control system
 - very large national shoe manufacturer
 - system gathers sales data daily from stores across Canada
- Data is used by following departments:
 - accounting
 - shipping
 - ordering
- Inventory functions are critical to the smooth operation of the system and the corporation.

Ethical decision making

- James is a quality assurance (QA) engineer with the software company
 - He suspects the inventory functions of the system are not sufficiently tested
 - However, they have passed all contracted tests.
- He is being pressured by his employers to sign off on the software.
- Legally he is only required to perform those tests which found their way into the contract
- However, his considerable experience in software testing leads him to be concerned over risks of incorrect system behavior

Ethical decision making

- Despite insisting, James' company states:
 - "We will go out of business if we do not deliver the software on time."
- James replies:
 - "If inventory subsystem fails, it will significantly harm our client and their employees."
- If the potential failure were to threaten lives, it would be clear to James that he should refuse to sign off
- However, given the reduced degree of threatened harm, James is faced by a difficult decision.

Applying the ACM Code

- This case highlights issues involving software risks.
- Principle 1.2 stress responsibility of computing professional to avoid harm for others
 - Principle 1.1 requires concern for human well-being
 - Principle 1.3 mandates professional integrity
 - Principle 2.1 defines quality as an ethical responsibility
- These principles may conflict with agreements and commitments of an employee to the employer and client.

Applying the ACM Code

- The ethical imperatives of the code suggest that:
 - James should not deliver a product he believes to be inferior
 - nor should he mislead the client about the quality of the product (1.3)
- He should continue to test, and has been told of the financial repercussions of not delivering the system.
 - At the very least, the client should be informed of his reservations.

Ethical decision making

- Armand is negotiating a contract with a local municipality
- Designing their traffic control system (TCS)
- He recommends they select the TCS system out of several available system on the market.
- Armand fails to mention that he is a major stockholder of the company producing TCS software.

Applying the ACM Code:

- This case highlights issues involving conflicts of interest.
- Principle 2.5: computer professionals must “strive to be perceptive, thorough and objective when evaluating, recommending and presenting system descriptions and alternatives.”
- Principle 1.3: implies a computer professional must be honest about “any circumstances that might lead to conflicts of interest”
 - IT professionals have special skills
 - It is their responsibility to ensure clients are fully aware of the options.
 - Also their responsibility to ensure professional recommendations are not modified for personal gain.

Ethical decision making

- Matthew is working on a project for his computer science course.
- Instructor has allotted a fix amount of computer time for the project.
 - This time is enforced by the computer system.
- Matthew runs out of time, but has not yet finished the project.
- Instructor cannot be reached.



Ethical decision making

- Matthew worked last year as a co-op programmer in the department.
- He is very familiar with procedures used to increase time allocations to accounts.
- Using what he learned last year, he is able to access the master account.
- Then he gives himself additional time.
- He now completes his project.

Applying the ACM code

- Principle 1.5 (property rights) has been violated.
- Principle 2.8: specifies that ACM members should “access communication resources only when authorized to do so”.
- By violating 2.8, Matthew is also violating Principle 2.3 (“know and respect existing laws”)
- As a student member of the ACM, Matthew must follow the code of ethics...
- ... even if he does not consider himself a computing professional.

Case Study: The Therac-25

Therac-25 Radiation Overdoses:

- Massive overdoses of radiation were given; the machine said no dose had been administered at all
- Caused severe and painful injuries and the death of three patients
- Important to study to avoid repeating errors
- Manufacturer, computer programmer, and hospitals/clinics all have some responsibility

Case Study: The Therac-25 (cont.)

Software and Design problems:

- Re-used software from older systems, unaware of bugs in previous software
- Weaknesses in design of operator interface
- Inadequate test plan
- Bugs in software
 - Allowed beam to deploy when table not in proper position
 - Ignored changes and corrections operators made at console

Case Study: The Therac-25 (cont.)

Why So Many Incidents?

- Hospitals had never seen such massive overdoses before, were unsure of the cause
- Manufacturer said the machine could not have caused the overdoses and no other incidents had been reported (which was untrue)
- The manufacturer made changes to the turntable and claimed they had improved safety after the second accident. The changes did not correct any of the causes identified later

Case Study: The Therac-25 (cont.)

Why So Many Incidents? (cont.)

- Recommendations were made for further changes to enhance safety; the manufacturer did not implement them
- The FDA declared the machine defective after the fifth accident
- The sixth accident occurred while the FDA was negotiating with the manufacturer on what changes were needed

Case Study: The Therac-25 (cont.)

Observations and Perspective:

- Minor design and implementation errors usually occur in complex systems; they are to be expected
- The problems in the Therac-25 case were not minor and suggest irresponsibility
- Accidents occurred on other radiation treatment equipment without computer controls when the technicians:
 - Left a patient after treatment started to attend a party
 - Did not properly measure the radioactive drugs
 - Confused micro-curies and milli-curies

System Quality

- Bug-free software is difficult to produce
- It must be carefully designed, developed, and tested
- Mistakes generated by computers can be far reaching
- Commenting and documenting software is required for effective maintenance throughout the life of the program



System Quality

ETHICAL ISSUES:

When is software, system or service ready for release?

SOCIAL ISSUES:

Can people trust quality of software, systems, services, data?

POLITICAL ISSUES:

Should congress or industry develop standards for software, hardware, data quality?

Is technology Good or Evil?



