3

Legal, Ethical, and Professional Issues in Information Security

In civilized life, law floats in a sea of ethics.

EARL WARREN, CHIEF JUSTICE, U.S. SUPREME COURT, 12 NOVEMBER 1962

PRINCIPLES of INFORMATION SECURITY

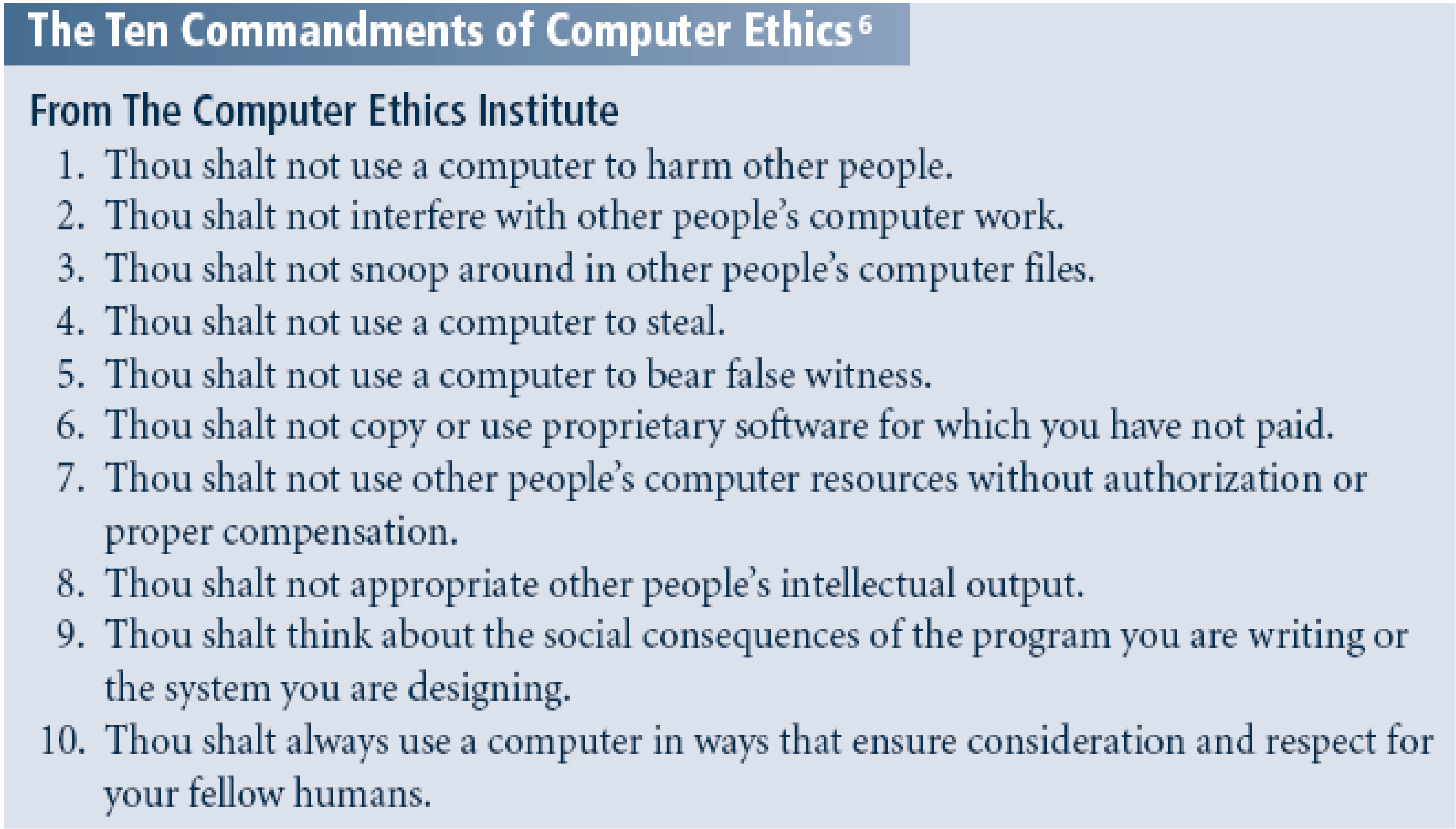
Introduction

- You must understand scope of an organization’s legal and ethical responsibilities
- To minimize liabilities/reduce risks, the information security practitioner must:
  - Understand **Laws compared to Ethics**
  - Stay current with **relevant US laws**
  - Watch for new issues that emerge in **Ethics and Information Security**

Law and Ethics in Information Security

- **Laws**: rules that mandate or prohibit certain societal behavior
- **Ethics**: define socially acceptable behavior
- **Cultural mores**: fixed moral attitudes or customs of a particular group; ethics based on these
- Laws carry sanctions of a governing authority; ethics do not

Example: Ethics in an Organization



The Ten Commandments of Computer Ethics[6]

From The Computer Ethics Institute

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

Policy versus Law

- **Policies**: body of expectations that describe acceptable and unacceptable employee behaviors in the workplace
- Policies function as laws within an organization; must be crafted carefully to ensure they are complete, appropriate, fairly applied to everyone
- Difference between policy and law: ignorance of a policy is an acceptable defense

Policy versus Law

Criteria for policy enforcement:

- Dissemination (distribution),
- Review (reading),
- Comprehension (understanding),
- Compliance (agreement),
- Uniform enforcement

Relevant U.S. Laws

- United States has been a leader in the development and implementation of information security legislation
- Implementation of information security legislation contributes to a more reliable business environment and a stable economy
- U.S. has demonstrated understanding of problems facing the information security field; has specified penalties for individuals and organizations failing to follow requirements set forth in U.S. civil statutes

Relevant U.S. Laws

Privacy

- One of the hottest topics in information security
- Is a “state of being free from unsanctioned intrusion”
- Ability to aggregate data from multiple sources allows creation of information databases previously unheard of

1. Federal Privacy Act 1974:
2. The Electronic Communication Privacy Act 1986
3. HIPPA 1996

Identity Theft

- Federal Trade Commission: FTC “occurring when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes”
- In US law: person commit identity theft got penalties range from 1 to 25 years in prison and fines.

Relevant U.S. Laws

Identity Theft

- FTC recommend people exposed to Identity theft to do the following steps

1) Report to reporting companies
2) If you know which account is attacked close it immediately
3) Register your case with FTC
4) Report incident with your local police office.

Relevant U.S. Laws

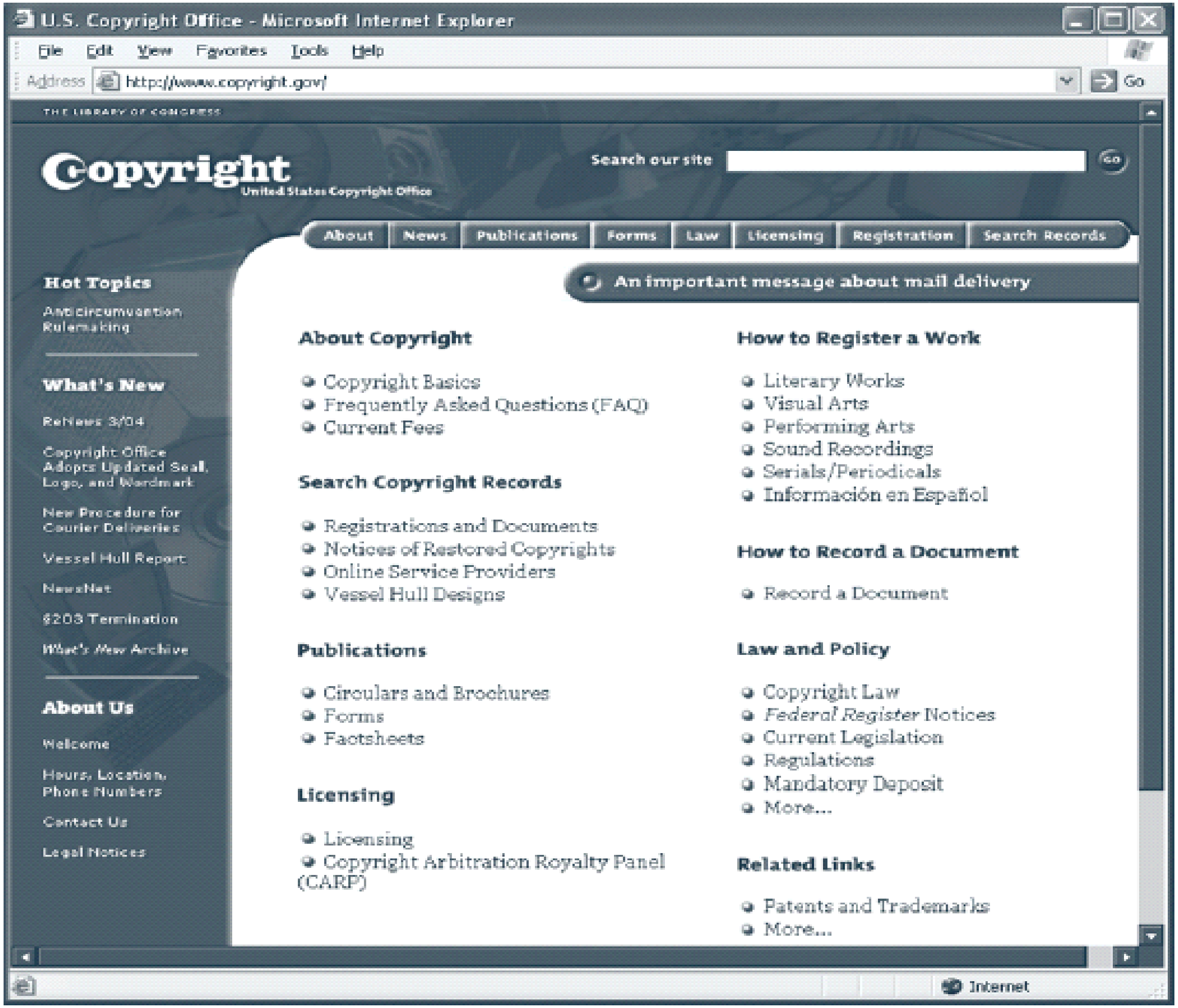
U.S. Copyright Law

- Intellectual property recognized as protected asset in the U.S.; copyright law extends to electronic formats

- With proper acknowledgment, permissible to include portions of others’ work as reference

- U.S. Copyright Office Web site: www.copyright.gov

Relevant U.S. Laws


U.S. Copyright Office - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://www.copyright.gov/
Go
THE LIBRARY OF CONGRESS
Copyright
United States Copyright Office
Search our site
GO
About News Publications Forms Law Licensing Registration Search Records
Internet

Hot Topics

Anticircumvention Rulemaking

What's New

ReNews 3/04

Copyright Office Adopts Updated Seal, Logo, and Wordmark

New Procedure for Courier Deliveries

Vessel Hull Report

NewsNet

§203 Termination

What's New Archive

About Us

Welcome

Hours, Location, Phone Numbers

Contact Us

Legal Notices

An important message about mail delivery

About Copyright

- Copyright Basics
- Frequently Asked Questions (FAQ)
- Current Fees

Search Copyright Records

- Registrations and Documents
- Notices of Restored Copyrights
- Online Service Providers
- Vessel Hull Designs

Publications

- Circulars and Brochures
- Forms
- Factsheets

Licensing

- Licensing
- Copyright Arbitration Royalty Panel (CARP)

How to Register a Work

- Literary Works
- Visual Arts
- Performing Arts
- Sound Recordings
- Serials/Periodicals
- Información en Español

How to Record a Document

- Record a Document

Law and Policy

- Copyright Law
- *Federal Register* Notices
- Current Legislation
- Regulations
- Mandatory Deposit
- More...

Related Links

- Patents and Trademarks
- More...

FIGURE 3-2 The U.S. Copyright Office Web Site

Relevant U.S. Laws

State and Local Regulations

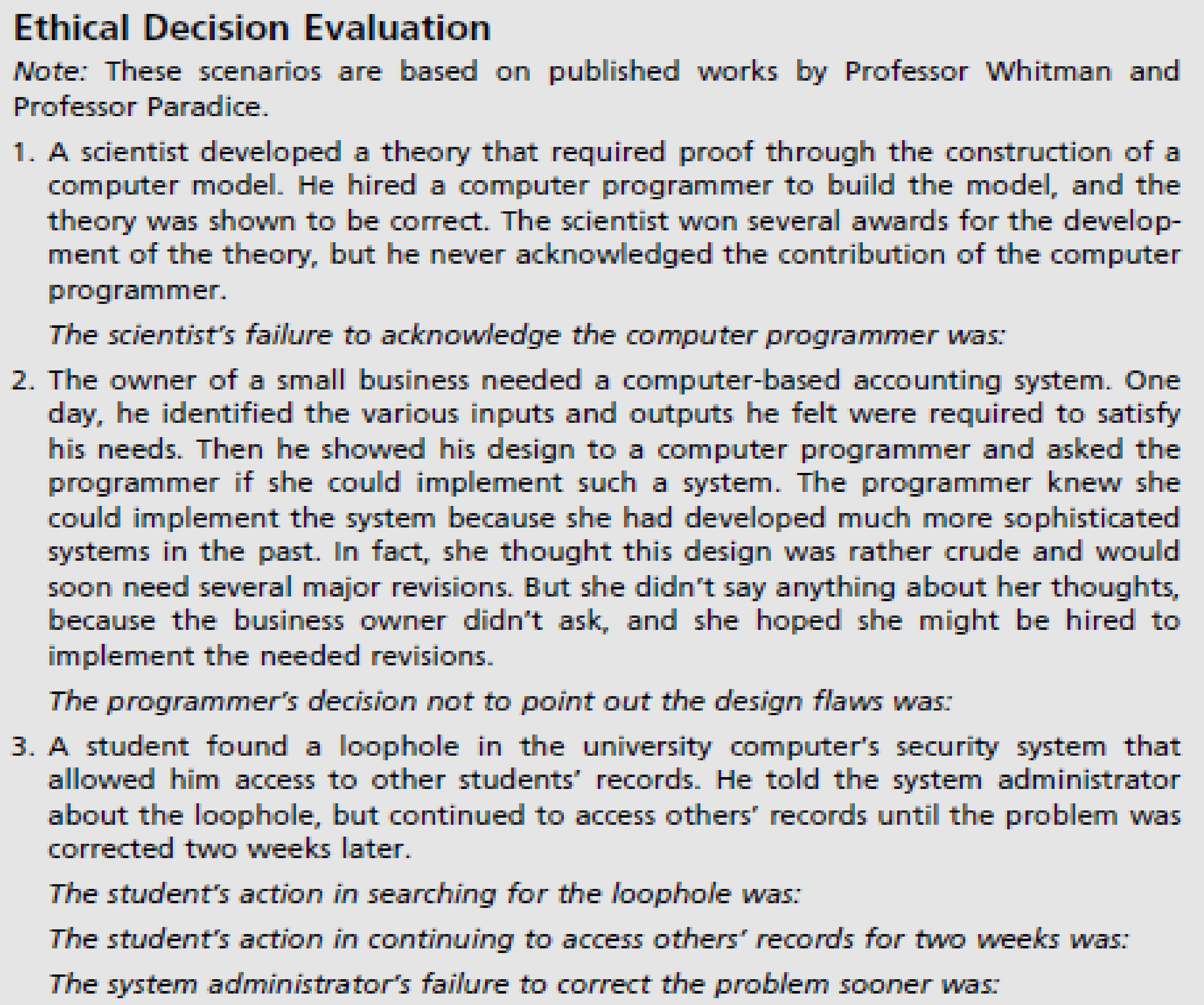
- Restrictions on organizational computer technology use exist at international, national, state, local levels
- Information security professional responsible for understanding state regulations and ensuring organization is compliant with regulations

International Laws and Legal Bodies

- IT professionals and IS practitioners should realize that when organizations do business on the Internet, they do business globally
- Professionals must be sensitive to laws and ethical values of many different cultures, societies, and countries
- Because of political complexities of relationships among nations and differences in culture, there are few international laws relating to privacy and information security
- These international laws are important but are limited in their enforceability

Ethical Differences Across Cultures

- Cultural differences create difficulty in determining what is and is not ethical
- Difficulties arise when one nationality’s ethical behavior conflicts with ethics of another national group
- **Example**: many of the ways in which Asian cultures use computer technology is considered software piracy by other nations
- In the following three pages you need to answer each question either with **(Very ethical, Ethical, neutral , unethical, Very unethical)**



Ethical Decision Evaluation

Note: These scenarios are based on published works by Professor Whitman and Professor Paradice.

1. A scientist developed a theory that required proof through the construction of a computer model. He hired a computer programmer to build the model, and the theory was shown to be correct. The scientist won several awards for the development of the theory, but he never acknowledged the contribution of the computer programmer.

   The scientist's failure to acknowledge the computer programmer was:

2. The owner of a small business needed a computer-based accounting system. One day, he identified the various inputs and outputs he felt were required to satisfy his needs. Then he showed his design to a computer programmer and asked the programmer if she could implement such a system. The programmer knew she could implement the system because she had developed much more sophisticated systems in the past. In fact, she thought this design was rather crude and would soon need several major revisions. But she didn't say anything about her thoughts, because the business owner didn't ask, and she hoped she might be hired to implement the needed revisions.

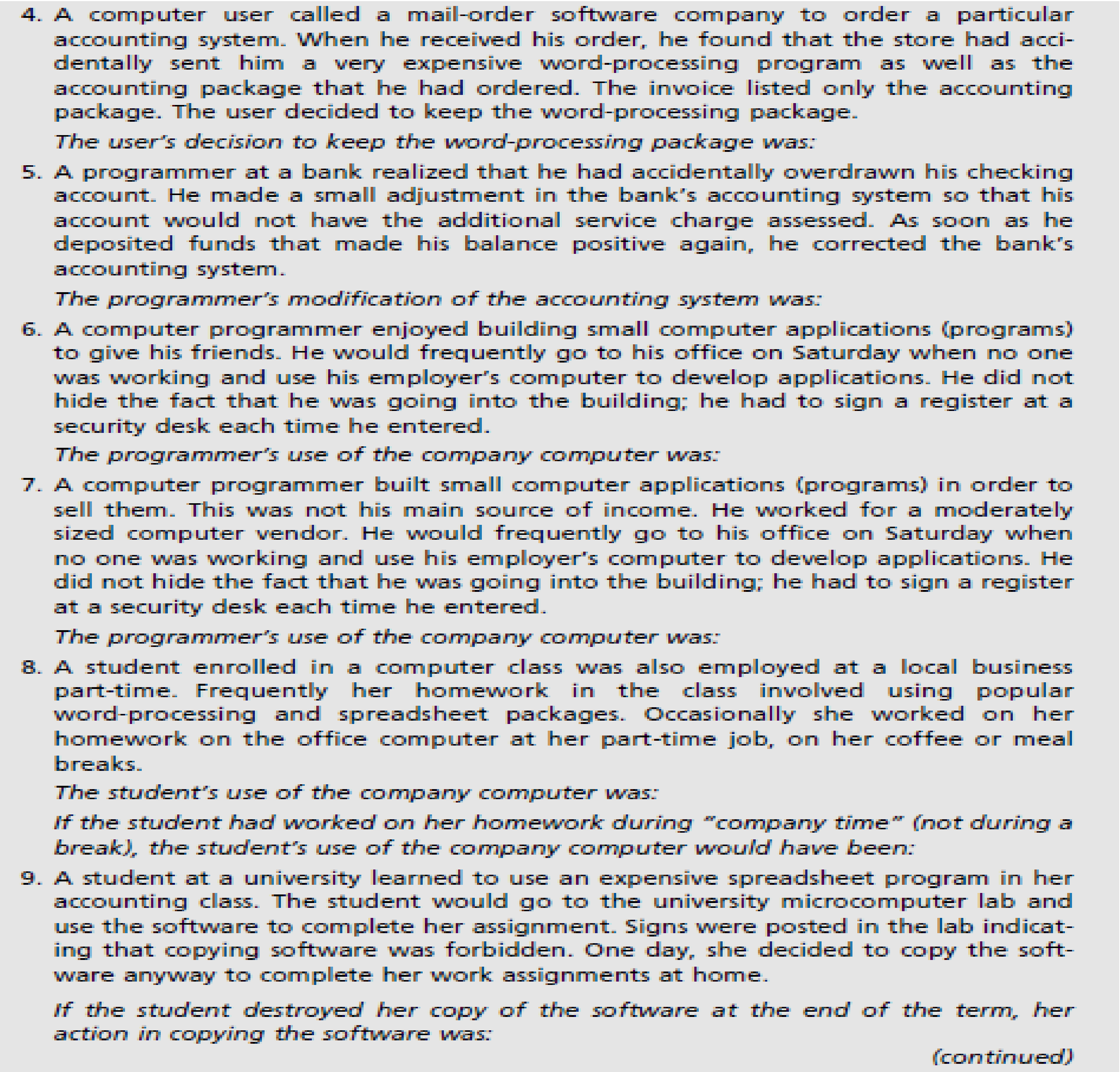
   The programmer's decision not to point out the design flaws was:

3. A student found a loophole in the university computer's security system that allowed him access to other students' records. He told the system administrator about the loophole, but continued to access others' records until the problem was corrected two weeks later.

   The student's action in searching for the loophole was:

   The student's action in continuing to access others' records for two weeks was:

   The system administrator's failure to correct the problem sooner was:



4. A computer user called a mail-order software company to order a particular accounting system. When he received his order, he found that the store had accidentally sent him a very expensive word-processing program as well as the accounting package that he had ordered. The invoice listed only the accounting package. The user decided to keep the word-processing package.

   The user's decision to keep the word-processing package was:

5. A programmer at a bank realized that he had accidentally overdrawn his checking account. He made a small adjustment in the bank's accounting system so that his account would not have the additional service charge assessed. As soon as he deposited funds that made his balance positive again, he corrected the bank's accounting system.

   The programmer's modification of the accounting system was:

6. A computer programmer enjoyed building small computer applications (programs) to give his friends. He would frequently go to his office on Saturday when no one was working and use his employer's computer to develop applications. He did not hide the fact that he was going into the building; he had to sign a register at a security desk each time he entered.

   The programmer's use of the company computer was:

7. A computer programmer built small computer applications (programs) in order to sell them. This was not his main source of income. He worked for a moderately sized computer vendor. He would frequently go to his office on Saturday when no one was working and use his employer's computer to develop applications. He did not hide the fact that he was going into the building; he had to sign a register at a security desk each time he entered.

   The programmer's use of the company computer was:

8. A student enrolled in a computer class was also employed at a local business part-time. Frequently her homework in the class involved using popular word-processing and spreadsheet packages. Occasionally she worked on her homework on the office computer at her part-time job, on her coffee or meal breaks.

   The student's use of the company computer was:

   If the student had worked on her homework during "company time" (not during a break), the student's use of the company computer would have been:

9. A student at a university learned to use an expensive spreadsheet program in her accounting class. The student would go to the university microcomputer lab and use the software to complete her assignment. Signs were posted in the lab indicating that copying software was forbidden. One day, she decided to copy the software anyway to complete her work assignments at home.

   If the student destroyed her copy of the software at the end of the term, her action in copying the software was:

(continued)

If the student forgot to destroy her copy of the software at the end of the term, her action in copying the software was:

If the student never intended to destroy her copy of the software at the end of the term, her action in copying the software was:

10. A student at a university found out that one of the local computer bulletin boards contained a "pirate" section (a section containing a collection of illegally copied software programs). He subscribed to the board, and proceeded to download several games and professional programs, which he then distributed to several of his friends.

    The student's actions in downloading the games were:

    The student's actions in downloading the programs were:

    The student's actions in sharing the programs and games with his friends were:

11. State College charges its departments for computer time usage on the campus mainframe. A student had access to the university computer system because a class she was taking required extensive computer usage. The student enjoyed playing games on the computer, and frequently had to request extra computer funds from her professor in order to complete her assignments.

    The student's use of the computer to play games was:

12. An engineer needed a program to perform a series of complicated calculations. He found a computer programmer capable of writing the program, but would only hire the programmer if he agreed to share any liability that may result from an error in the engineer's calculations. The programmer said he would be willing to assume any liability due to a malfunction of the program, but was unwilling to share any liability due to an error in the engineer's calculations.

    The programmer's position in this situation is:

    The engineer's position in this situation is:

13. A manager of a company that sells computer-processing services bought similar services from a competitor. She used her access to the competitor's computer to try to break the security system, identify other customers, and cause the system to "crash" (cause loss of service to others). She used the service for over a year and always paid her bills promptly.

    The manager's actions were:

14. One day, a student programmer decided to write a virus program. Virus programs usually make copies of themselves on other disks automatically, so the virus can spread to unsuspecting users. The student wrote a program that caused the microcomputer to ignore every fifth command entered by a user. The student took his program to the university computing lab and installed it on one of the microcomputers. Before long, the virus spread to hundreds of users.

    The student's action of infecting hundreds of users' disks was:

    If the virus program output the message "Have a nice day," then the student's action of infecting hundreds of users' disks would have been:

    If the virus erased files, then the student's action of infecting hundreds of users' files would have been:

Ethics and Education

- Overriding factor in leveling ethical perceptions within a small population is education
- Employees must be trained in expected behaviors of an ethical employee, especially in areas of information security
- Proper ethical training vital to creating informed, well prepared, and low-risk system user

Deterrence to Unethical and Illegal Behavior

- Three general causes of unethical and illegal behavior: **ignorance**, **accident**, **intent**
- **Deterrence**: best method for preventing an illegal or unethical activity; e.g., laws, policies, technical controls
- Laws and policies only deter if three conditions are present:
  - **Fear of penalty**
  - **Probability of being caught**
  - **Probability of penalty being administered**

Codes of Ethics and Professional Organizations

- Several professional organizations have established codes of conduct/ethics
- Codes of ethics can have positive effect; unfortunately, many employers do not encourage joining these professional organizations
- Responsibility of security professionals to act ethically and according to policies of employer, professional organization, and laws of society

Summary

- Laws: rules that mandate or prohibit certain behavior in society; drawn from ethics
- Ethics: define socially acceptable behaviors; based on cultural mores (fixed moral attitudes or customs of a particular group)
- Types of law: civil, criminal, private, public

Summary (continued)

- Many organizations have codes of conduct and/or codes of ethics
- Organization increases liability if it refuses to take measures known as due care
- Due diligence requires that organization make valid effort to protect others and continually maintain that effort