SECURITY IN COMPUTING, FIFTH EDITION

Chapter 11: Legal Issues and Ethics

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Chapter 11 Objectives

- Learn about copyrights, patents, and trade secrets and their roles in software protection
- Describe how information is different from other assets
- Examine relationships between employees and employers in the context of software development
- Understand vendor responsibilities and responsible vulnerability disclosure
- Learn about a variety of computer security–relevant legal statutes
- Explore ethics in a computer security and privacy context

Laws and Ethics

- The legal system has adapted quite well to computer technology
- However, fixing a problem through the courts can be time consuming
- Also, technology continuously evolving
  - Law may lag technology

Laws and Ethics

- Ethics does not need to change
  - Typically more situational than personal
- Privacy strongly related to legal and ethical issues
  - Enforcing may be legal, ethics provides general guidelines

Laws and Ethics

- Laws related to computer security:
  - Affect individual's right to privacy and secrecy
  - Regulate the use, development, and ownership of data and programs
    - Protect proprietary programs, motivation to develop new tools
  - Define legal remedies to protect the secrecy, integrity, and availability of computer information and service

Motivation

- Know what protection the law provides for computers and data
- Appreciate laws that protect the rights of others with respect to computers, programs, and data
- Understand existing laws as a basis for recommending new laws to protect computers, data, and people

Aspects of Computer Security Legal Protection

- Protecting computing systems against criminals
  - Computer criminals violate the principles of confidentiality, integrity, and availability for computer systems
  - Better to prevent than prosecute
    - However, legal punishment help deter future violations
    - Compensation to injured parties

Aspects of Computer Security Legal Protection

- Protecting code and data
  - Through Copyrights, patents, and trade secrets
- Protecting programmers' and employers' rights
  - Legal rights of employees and employers vary
- Protecting users of programs
  - legal system should protect your rights as a consumer

Protecting Programs and Data

- Copyrights
  - Designed to protect the expression of ideas
  - Gives the author the exclusive right to make copies of the expression and sell them to the public
- Patents
  - Designed to protect inventions, tangible objects, or ways to make them
  - Patents were intended to apply to the results of science, technology, and engineering as opposed to arts and writing

Protecting Programs and Data

- Trade secrets
  - Information that gives one company a competitive advantage over others
  - Must be closely guarded as a secret, or legal protections are lost

Copyrights

- In the United States, copyright can be registered for original works of expression but not for ideas
- "Fair use" allows copyrighted material to be used in ways that do not interfere with author's rights:
  - criticism, comment, new reporting, teaching, scholarship, or research
- Software can be copyrighted
  - The code is protected but the algorithms are not
  - If source code is not published (i.e., only compiled code is published), copyright may not apply

Patents

- Novelty requirement
  - Cannot be obvious to a person ordinarily skilled in the relevant field
- Must convince the patent office that the invention deserves a patent (i.e., that it is novel)
- A patent holder must oppose all infringement or risk losing the patent rights
- Since 1981, patent law has extended to include computer software, recognizing that algorithms are inventions

Trade Secrets

- If someone obtains a trade secret improperly and profits from it, the owner can recover profits, damages, lost revenues, and legal costs
- If someone else happens to discover the secret independently, there is no infringement

Trade Secrets

- Reverse engineering a trade secret is not infringement
- Trade secrets can protect secret computer algorithms from being used in other products
  - Cannot provide legal protection against software piracy
  - The challenge of using trade secrets to protect software is that software can be effectively reverse engineered

Comparing Copyrights, Patents, and Trade Secrets

	Copyright	Patent	Trade Secret
Protects	Expression of idea, not idea itself	Invention—the way something works	A secret, competitive advantage
Protected object made public	Yes; intention is to promote publication	Design filed at Patent Office	No
Requirement to distribute	Yes	No	No
Ease of filing	Very easy, do-it-yourself	Very complicated; specialist lawyer suggested	No filing
Duration	Varies by country; approximately 75–100 years is typical	19 years	Indefinite
Legal protection	Sue if unauthorized copy sold	Sue if invention copied	Sue if secret improperly obtained

Special Characteristics of Information

- Like material goods, information is valuable
- Unlike material goods, information
  - Is not depletable
    - Can be sold again and again without diminishing quality
  - Can be replicated
    - After buyer bought the information, he can resell it
      - Deprive the original seller of further sales
  - Has a minimal marginal cost
    - Digital information reproduction costs less than published information
      - Copy can be perfect, indistinguished from the original

Special Characteristics of Information

- Like material goods, information is valuable
- Unlike material goods, information (cont.)
  - Often has a time-dependent value
    - Such as company information affecting stock price
  - Often transferred intangibly
    - Information may be changed without reader noticing
- All of these factors impact how information is treated under the law

Rights of Employees and Employers

- Ownership of a patent
  - An employer has the right to patent if the employee's job functions included inventing the product.
  - Even if an employee patents something, the employer can argue for a right to use the invention if the employer contributed some resources
- Ownership of a copyright
  - Similar to patent

Rights of Employees and Employers

- Licenses
  - In return for a fee, a programmer grants a company a license to use her program.
    - The license can include many factors, such as time period, number of users, number of systems, and so on
- Trade secret protection
  - A company owns the trade secrets of its business-confidential data.
    - As with copyrights and patents, an employer can argue about having contributed to the development of trade secrets

Reporting Software Flaws

- A proposed model for responsible vulnerability reporting:
  - The vendor must acknowledge a vulnerability report confidentially to the reporter.
  - The vendor must agree that the vulnerability exists (or argue otherwise) confidentially to the reporter.
  - The vendor must inform users of the vulnerability and any available countermeasures within 30 days or request additional time from the reporter as needed.

Reporting Software Flaws

- A proposed model for responsible vulnerability reporting (cont.):
  - After informing users, the vendor may request from the reporter a 30-day quiet period to allow users time to install patches.
  - At the end of the quiet period, the vendor and reporter should agree on a date at which time the vulnerability information may be released to the general public.

Reporting Software Flaws

- A proposed model for responsible vulnerability reporting (cont.):
  - The vendor should credit the reporter with having located the vulnerability.
  - If the vendor does not follow these steps, the reporter should work with a coordinator to determine a responsible way to publicize the vulnerability.

Reporting Software Flaws

- This model, as well as others like it, was created in response to a series of incidents
  - in which some vendors refused to patch disclosed vulnerabilities in reasonable time.
- Some software vendors still threaten vulnerability researchers with lawsuits
  - while others happily pay bounties for disclosure of vulnerabilities in their software

Computer Crime

- Rules of property
  - Most laws have evolved to recognize data and computer services as property.
- Rules of evidence
  - Demonstrating authenticity of computer-based evidence is a challenge.
  - Chain of custody: Law enforcement track clearly and completely the order and identity of people who had access to evidence in an effort to demonstrate that no one had the opportunity to tamper.

Computer Crime

- Threats to integrity and confidentiality
  - Laws have evolved to recognize breaches of privacy and damage to data as crimes.
- Value of data
  - Digital data, from a legal perspective, is now considered to be worth what a buyer would be willing to pay for it.

Computer Crime Is Hard to Prosecute

- Lack of domain understanding by courts, lawyers, law enforcement, and jurors
- Lack of physical evidence
- Lack of political impact because direct harm to people is harder to identify
- Complexity of cases

Computer Crime Is Hard to Prosecute

- Ages of defendants, who are more likely than many other serious criminals to be juvenile
- Even when there is clear evidence of a crime, the victim (e.g., banks) may not wish to prosecute
  - they may lose the trust of their customers

Example Computer Statutes

- US Freedom of Information Act
  - Provides public access to information collective by the executive branch of the US government
- US Privacy Act
  - Protects privacy of personal data collected by the government

Example Computer Statutes

- US Computer Fraud and Abuse Act
  - Prohibits computer fraud, trafficking in passwords, transmitting code that damages a system, unauthorized access to systems
- US Economic Espionage Act
  - Outlaws use of a computer for foreign espionage

Example Computer Statutes (cont.)

- US Electronic Communications Privacy Act
  - Protects against electronic wiretapping
- Gramm-Leach-Bliley Act
  - Requires financial institutions to undergo security risk assessments, adopt a program to protect customers' nonpublic personal information, and provide customers with privacy policies

Example Computer Statutes (cont.)

- HIPAA
  - Requires protection of the privacy of individuals' medical records
- USA Patriot Act
  - Gave law enforcement an easier path to obtaining wiretaps on potential foreign agents and made damaging computer systems a felony

Example Computer Statutes (cont.)

- The CAN SPAM Act
  - Bans deceptive email advertising, requires opt-out options
- California Breach Notification
  - Requires any company doing business in California to notify individuals of any breach that is reasonably believed to have compromised personal information of a California resident

Example Computer Statutes (cont.)

- Council of Europe Agreement on Cybercrime
  - Requires signing countries to define cybercrime activities and support their investigation and prosecution across national boundaries
- EU Data Protection Act
  - Established privacy rights and protection responsibilities for all citizens of member countries

Laws and Ethics

- Laws change in time and different locations
- What guidelines should they follow?
- Is there a difference between laws and ethics?
  - How laws always ethical?

Comparison of Law and Ethics

Law	Ethics
Described by formal, written documents	Described by unwritten principles
Interpreted by courts	Interpreted by each individual
Established by legislatures representing all people	Presented by philosophers, religions, professional groups
Applied to everyone	Chosen personally
Priority determined by courts if two laws conflict	Priority determined by an individual if two principles conflict
"Right" arbitrated finally by court	Not arbitrated externally
Enforced by police and courts	Enforced by intangibles such as principles and beliefs

Examining a Situation for Ethical Issues

- Understand the situation
- Know several theories of ethical reasoning
- List the ethical principles involved
- Determine which principles outweigh others
- Make and defend an ethical choice

Bases of Ethical Theories

	Consequence-Based	Rule-Based
Individual	based on consequences to individual	based on rules acquired by the individual—from religion, experience, analysis
Universal	based on consequences to all of society	based on universal rules, evident to everyone

Bases of Ethical Theories

- The **teleological** theory of ethics focuses on the consequences of an action.
- The action to be chosen is the one that results in the greatest future good and the least harm.
- There are 2 important forms:
  - Egoism: a moral judgment is based on the positive benefits to the person taking the action
  - Utilitarianism: an assessment of good and bad results for the entire universe

Bases of Ethical Theories

- For example, if a fellow student asks you to write a program he was assigned for a class, you might consider the good against the bad
  - Good: he will owe you a favor
  - Bad: you might get caught, causing embarrassment and possible disciplinary action, plus your friend will not learn the techniques to be gained from writing the program, leaving him deficient.

Bases of Ethical Theories

- **Rule-deontology** is the school of ethical reasoning that believes certain universal, self-evident, natural rules specify our proper conduct.
  - Defines **Universalism**
- Certain basic moral principles are adhered to because of our responsibilities to one another
- These principles are often stated as rights:
  - the right to know,
  - the right to privacy,
  - the right to fair compensation for work.

Situation I: Use of Computer Services

- Dave works as a programmer for a large software company. He writes and tests utility programs such as compilers.
- His company operates two computing shifts:
  - During the day, program development and online applications are run;
  - at night, batch production jobs are completed.

Situation I: Use of Computer Services

- Dave has access to workload data and learns that the evening batch runs are complementary to daytime programming tasks
  - that is, adding programming work during the night shift would not adversely affect performance of the computer to other users.

Situation I: Use of Computer Services

- Dave comes back after normal hours to develop a program to manage his own stock portfolio.
- His drain on the system is minimal, and he uses very few expendable supplies, such as printer paper.
- Is Dave's behavior ethical?

Situation I: Use of Computer Services

- The utilitarian would consider the total excess of good over bad for all people:
  - Dave receives benefit from use of computer time, although for this application the amount of time is not large.
  - Dave has a possibility of punishment, but he may rate that as unlikely.
  - The company is neither harmed nor helped by this activity.
  - Thus, the utilitarian could argue that Dave's use is justifiable.

Situation I: Use of Computer Services

- The universalism principle seems as if it would cause a problem because, clearly, if everyone did this, quality of service would degrade.
  - Each new user has to weigh good and bad separately.
  - Dave's use might not burden the system, and neither might Ann's
    - but when Bill wants to use the system, it is heavily enough used that Bill's use *would* affect other people.

Situation II: Privacy Rights

- Donald works for the county records department as a computer records clerk, where he has access to files of property tax records.
- For a scientific study, a researcher, Ethel, has been granted access to the numerical portion—but not the corresponding names—of some records.

Situation II: Privacy Rights

- Ethel finds some information that she would like to use, but she needs the names and addresses corresponding with certain properties.
- Ethel asks Donald to retrieve the names and addresses so she can contact these people for more information and for permission to do further study.
- Should Donald release the names and addresses?

Situation II: Privacy Rights

- A rule-deontologist would argue that privacy is an inherent good and that one should not violate the privacy of another.
- Therefore, Donald should not release the names.

Situation III: Denial of Service

- Charlie and Carol are students at a university in a computer science program
  - Each writes a program for a class assignment.
- Charlie's program happens to uncover a flaw in a compiler that ultimately causes the entire computing system to fail
  - all users lose the results of their current computation.

Situation III: Denial of Service

- Charlie's program uses acceptable features of the language
  - the compiler is at fault.
- Charlie did not suspect his program would cause a system failure
  - He reports the program to the computing center and tries to find ways to achieve his intended result without exercising the system flaw.

Situation III: Denial of Service

- The system continues to fail periodically, for a total of 10 times (beyond the first failure).
  - When the system fails, sometimes Charlie is running a program, but sometimes Charlie is not.
- The director contacts Charlie, who shows all his program versions to the computing center staff.
  - The staff concludes that Charlie may have been inadvertently responsible for some, but not all, of the system failures
    - but that his latest approach to solving the assigned problem is unlikely to lead to additional system failures.

Situation III: Denial of Service

- On further analysis, the computing center director notes that Carol has had programs running each of the first eight (of 10) times the system failed.
- The director uses administrative privilege to inspect Carol's files
  - finds a file that exploits the same vulnerability as did Charlie's program.
- The director immediately suspends Carol's account
  - denying Carol access to the computing system.
- => Carol is unable to complete assignment on time
  - she receives a D in the course, and she drops out of school.

Situation III: Denial of Service

- In this situation the choices are not obvious.
- The situation is presented as a completed scenario
  - Can you suggest suggest alternative actions the players *could have taken?*
    - In this way, you build a repertoire of actions that you can consider in similar situations that might arise.

Situation IV: Ownership of Programs

- Greg is a programmer working for a large aerospace firm, Star Computers, which works on many government contracts
- Cathy is Greg's supervisor.
- Greg is assigned to program various kinds of simulations.

Situation IV: Ownership of Programs

- To improve his programming abilities, Greg writes some programming tools, such as a cross-reference facility and a program that automatically extracts documentation from source code.
  - These are not assigned tasks for Greg
    - he writes them independently and uses them at work, but he does not tell anyone about them
  - Greg has written them in the evenings, at home, on his personal computer.

Situation IV: Ownership of Programs

- Greg decides to market these programming aids by himself.
- When Star's management hears of this, Cathy is instructed to tell Greg that he has no right to market these products
  - when he was employed, he signed a form stating that all inventions become the property of the company.

Situation IV: Ownership of Programs

- Cathy does not agree with this position
  - she knows that Greg has done this work on his own
  - She reluctantly tells Greg that he cannot market these products
    - She also asks Greg for a copy of the products.

Situation IV: Ownership of Programs

- Cathy quits working for Star and takes a supervisory position with Purple Computers, a competitor of Star.
- She takes with her a copy of Greg's products and distributes it to the people who work with her.
- These products are so successful that they substantially improve the effectiveness of her employees
  - Cathy is praised by her management and receives a healthy bonus.

Situation IV: Ownership of Programs

- Greg hears of this, and contacts Cathy
- Cathy contends that because the product was determined to belong to Star and because Star worked largely on government funding, the products were really in the public domain
  - and therefore they belonged to no one in particular.

Situation IV: Ownership of Programs

- This story certainly has major legal implications.
- Virtually everyone could sue everyone else
  - depending on the amount they are willing to spend on legal expenses, they could keep the cases in the courts for several years.
  - Probably no judgment would satisfy all.

Situation IV: Ownership of Programs

- Let us set aside the legal aspects and look at the ethical issues.
- We want to determine who might have done what
  - and what changes might have been possible to prevent a tangle for the courts to unscramble.

Situation IV: Ownership of Programs

- Let us explore the principles involved:
  - Rights. What are the respective rights of Greg, Cathy, Star, and Purple?
  - Basis. What gives Greg, Cathy, Star, and Purple those rights? What principles of fair play, business, property rights, and so forth are involved in this case?

Situation IV: Ownership of Programs

- Let us explore the principles involved (cont.):
  - Priority. Which of these principles are inferior to which others? Which ones take precedence?
    - it may be impossible to compare two different rights, so the outcome of this analysis may yield some rights that are important but that cannot be ranked first, second, third.
  - Additional information. What additional facts do you need in order to analyze this case? What assumptions are you making in performing the analysis?

Situation V: Proprietary Resources

- Suzie owns a copy of G-Whiz, a proprietary software package she purchased legitimately
- The software is copyrighted
  - the documentation contains a license agreement that says that the software is for use by the purchaser only.
- Suzie invites Luis to look at the software to see if it will fit his needs.
- Luis goes to Suzie's computer and she demonstrates the software to him.
  - He says he likes what he sees, but he would like to try it in a longer test.

Situation V: Proprietary Resources

- The potential next steps are where ethical responsibilities arise:
  - Suzie offers to copy the disk for Luis to use.
  - Suzie copies the disk for Luis to use
    - Luis uses it for some period of time.
  - Suzie copies the disk for Luis to use
    - Luis uses it for some period of time and then buys a copy for himself.

Situation V: Proprietary Resources

- The potential next steps are where ethical responsibilities arise:
  - Suzie copies the disk for Luis to try out overnight, under the restriction that he must bring the disk back to her tomorrow and must not copy it for himself.
    - Luis does so.
  - Suzie copies the disk with the same restrictions, but Luis makes a copy for himself before returning it to Suzie.

Situation V: Proprietary Resources

- The potential next steps are where ethical responsibilities arise (cont.):
  - Suzie copies the disk with the same restrictions, and Luis makes a copy for himself, but he then purchases a copy.
  - Suzie copies the disk with the same restrictions, but Luis does not return it.

Situation VI: Fraud

- Alicia works as a programmer in a corporation.
- Ed, her supervisor, tells her to write a program to allow people to post entries directly to the company's accounting files ("the books").
- Alicia knows that ordinarily programs that affect the books involve several steps
  - all of which have to balance.

Situation VI: Fraud

- Alicia realizes that with the new program, it will be possible for one person to make changes to crucial amounts
  - there will be no way to trace who made these changes, with what justification, or when.
- Alicia raises these concerns to Ed, who tells her not to be concerned
  - that her job is simply to write the programs as he specifies.

Situation VI: Fraud

- He says that he is aware of the potential misuse of these programs
  - he justifies his request by noting that periodically a figure is mistakenly entered in the books and the company needs a way to correct the inaccurate figure.

Situation VI: Fraud

- Analysis:
- The act-deontologist would say that truth is good.
  - Therefore, if Alicia thought the purpose of the program was to deceive, writing it would not be a good act
    - If the purpose were for learning or to be able to admire beautiful code, then writing it might be justifiable.

Situation VI: Fraud

- Analysis:
- A more useful analysis is from the perspective of the utilitarian.
- To Alicia, writing the program brings possible harm for being an accomplice to fraud, with the gain of having cooperated with her manager.
  - She has a possible item with which to blackmail Ed
    - but Ed might also turn on her and say the program was her idea.
  - On balance, this option seems to have a strong negative slant.

Situation VI: Fraud

- Analysis:
- By not writing the program, her possible harm is being fired.
- However, she has a potential gain by being able to “blow the whistle” on Ed.
  - This option does not seem to bring her much good, either.

Situation VI: Fraud

- Analysis:
- But fraudulent acts have negative consequences for the stockholders, the banks, and other innocent employees.
- Not writing the program brings only personal harm to Alicia, which is similar to the harm described earlier.
  - Thus, it seems as if not writing the program is the more positive option.

Situation VI: Fraud

- Analysis:
- There is another possibility:
  - The program may *not* be for fraudulent purposes. If so, then there is no ethical conflict.
  - Therefore, Alicia might try to determine whether Ed's motives are fraudulent.

Situation VII: Accuracy of Information

- Emma is a researcher at an institute where Paul is a statistical programmer.
- Emma wrote a grant request to a cereal manufacturer
  - to show the nutritional value of a new cereal, Raw Bits.
  - The manufacturer funded Emma's study.
- Emma is not a statistician
  - She has brought all of her data to Paul to ask him to perform appropriate analyses and to print reports for her to send to the manufacturer.
- Unfortunately, the data Emma has collected seem to refute the claim that Raw Bits is nutritious, and, in fact, they may indicate that Raw Bits is harmful.

Situation VII: Accuracy of Information

- Paul presents his analyses to Emma
  - also indicates that some other correlations could be performed that would cast Raw Bits in a more favorable light.
- Paul makes a facetious remark about his being able to use statistics to support either side of any issue.

Situation VII: Accuracy of Information

- Analysis:
  - Clearly, if Paul changed data values in this study, he would be acting unethically.
  - However, if data used as is, some questions arise:
    - Is it any more ethical for him to suggest analyzing correct data in a way that supports two or more different conclusions?
    - Is Paul obligated to present both the positive and the negative analyses?
    - Is Paul responsible for the use to which others put his program results?

Situation VII: Accuracy of Information

- Analysis (cont.):
  - If Emma does not understand statistical analysis, is she acting ethically in accepting Paul's positive conclusions?
    - His negative conclusions?
  - Emma suspects that if she forwards negative results to the manufacturer, they will just find another researcher to do another study.
    - She suspects that if she forwards both sets of results to the manufacturer, they will publicize only the positive ones.

Situation VII: Accuracy of Information

- Analysis (cont.):
  - What ethical principles support her sending both sets of data?
    - What principles support her sending just the positive set? What other courses of action has she?

Situation VIII: Ethics of Hacking or Cracking

- Goli is a computer security consultant; she enjoys the challenge of finding and fixing security vulnerabilities.
- Independently wealthy, she does not need to work
  - she has ample spare time in which to test the security of systems.

Situation VIII: Ethics of Hacking or Cracking

- In her spare time, Goli does three things:
  - First, she aggressively attacks commercial products for vulnerabilities.
    - She is quite proud of the tools and approach she has developed, and she is quite successful at finding flaws.
  - Second, she probes accessible systems on the Internet, and when she finds vulnerable sites, she contacts the owners to offer her services repairing the problems.

Situation VIII: Ethics of Hacking or Cracking

- In her spare time, Goli does three things (cont.):
  - Finally, she is a strong believer in high-quality pastry, and she plants small programs to slow performance in the websites of pastry shops that do not use enough butter in their pastries.
- Let us examine these three actions in order.

Situation VIII: Ethics of Hacking or Cracking

- Analysis:
- Vulnerabilities in Commercial Products
  - We have already described a current debate regarding the vulnerability reporting process
    - Now let us explore the ethical issues involved in that debate.
  - Clearly, from a rule-based ethical theory, attackers are wrong to perform malicious attacks.
  - The appropriate theory seems to be one of consequence:
    - Who is helped or hurt by finding and publicizing flaws in products?

Situation VIII: Ethics of Hacking or Cracking

- Analysis:
- Vulnerabilities in Commercial Products
  - Who is helped or hurt by finding and publicizing flaws in products?
    - Relevant parties are attackers,
    - the vulnerability finder, the vendor, and the using public.
    - Notoriety or credit for finding the flaw is a small interest.
    - The interests of the vendor (financial, public relations) are less important than the interests of users to have secure products.
      - But how are the interests of users best served?

Situation VIII: Ethics of Hacking or Cracking

- Analysis:
- *Full disclosure* helps users assess the seriousness of the vulnerability and apply appropriate protection.
- But it also gives attackers more information with which to formulate attacks.
- Early full disclosure—before the vendor has countermeasures ready—may actually harm users
  - by leaving them vulnerable to a now widely known attack.

Situation VIII: Ethics of Hacking or Cracking

- Analysis:
- *Partial disclosure*—the general nature of the vulnerability but not a detailed exploitation scenario—may forestall attackers.

Situation VIII: Ethics of Hacking or Cracking

- Analysis:
- *Partial disclosure*— One can argue that the vulnerability details are there to be discovered;
  - when a vendor announces a patch for an unspecified flaw in a product, the attackers will test that product aggressively
    - study the patch carefully to try to determine the vulnerability.
  - Attackers will then spread a complete description of the vulnerability to other attackers through an underground network
    - attacks will start against users who may not have applied the vendor's fix.

Situation VIII: Ethics of Hacking or Cracking

- Analysis:
- *No disclosure*. Perhaps users are best served by a scheme in which every so often new code is released
  - sometimes fixing security vulnerabilities, sometimes fixing things that are not security related, and sometimes adding new features
- But without a sense of significance or urgency, users may not install this new code.

Summary

- Copyrights, patents, and trade secrets all have roles to play in providing legal protection for software
- Important legal intricacies determine relationships among employees, employers, software vendors, and customers
- Statutes in a variety of overlapping jurisdictions may determine what computer crimes are, how they are investigated, and how they may be enforced
- Unlike legal issues, ethical issues have both personal and philosophical elements and therefore often lack clear answers

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.

Questions?

From *Security in Computing, Fifth Edition*, by Charles P. Pfleeger, et al. (ISBN: 9780134085043). Copyright 2015 by Pearson Education, Inc. All rights reserved.