

LEGAL ISSUES AND ETHICS

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

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
- 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 the 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
- 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 replicated
 - Has a minimal marginal cost
 - Often has a time-dependent value
 - Often transferred intangibly
- 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
- 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.
 - 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.
 - 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.

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.
- 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
- 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 because they may lose the trust of their customers

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
- 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 (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
- 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
- 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

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

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. 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.
- 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 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.
- 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 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. 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.
- 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.
- 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 and 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. Because of this, Carol is unable to complete her assignment on time; she receives a D in the course, and she drops out of school.

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.
- 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.
- 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 since, when he was employed, he signed a form stating that all inventions become the property of the company. Cathy does not agree with this position because 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.
- 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, and Cathy is praised by her management and receives a healthy bonus. Greg hears of this, and contacts Cathy, who 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 V: Proprietary Resources

- Suzie owns a copy of G-Whiz, a proprietary software package she purchased legitimately. The software is copyrighted, and 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 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. Alicia realizes that with the new program, it will be possible for one person to make changes to crucial amounts, and 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. He says that he is aware of the potential misuse of these programs, but 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 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.
- Paul presents his analyses to Emma but 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 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, so she has ample spare time in which to test the security of systems.
- 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. 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.

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