

I. Introduction & Objectives

- This lecture focuses on the intersection of computer security, legal frameworks, and ethical considerations.
 - **Chapter 11 Objectives:**
 1. Understand **copyrights, patents, and trade secrets** for software protection.
 2. Recognize how **information differs** from traditional assets.
 3. Analyze **employee/employer relationships** concerning software development IP.
 4. Discuss **vendor responsibilities** and **responsible vulnerability disclosure**.
 5. Identify key **computer security legal statutes**.
 6. Explore **ethical dimensions** in computer security and privacy.
-

II. Protecting Programs and Data (Intellectual Property)

A. Copyrights

1. **Definition:** Designed to protect the **expression of ideas**, not the ideas themselves. Grants the author **exclusive rights** to copy and sell the expression.
2. **Scope (US):** Applies to **original works of expression**. Ideas, procedures, processes, systems, methods of operation, concepts, principles, or discoveries are *not* copyrightable per se.
3. **Software Protection:**
 - **Code is protected** (the specific way the algorithm is written).
 - **Algorithms themselves are not** protected by copyright (they are ideas/processes).
 - **► Clarification Needed:** The slide notes "If source code is not published (i.e., only compiled code is published), copyright may not apply." This needs further investigation, as copyright generally subsists automatically upon creation in a fixed medium, regardless of publication format. However, registration and enforcement might be affected.
4. **Fair Use Doctrine:**
 - **Definition:** Allows limited use of copyrighted material without permission for purposes like:
 - Criticism
 - Comment

- News reporting
- Teaching
- Scholarship
- Research
- **Key Factor:** Does the use interfere with the author's exclusive rights (e.g., market value)?
- **Real-world Example:** Quoting sections of a textbook in a research paper for critique.

B. Patents

1. **Definition:** Designed to protect **inventions**, tangible objects, or novel ways of making them. Focuses on **utility and novelty**.
2. **Scope:** Intended for results of science, technology, and engineering.
3. **Requirements:**
 - **Novelty:** The invention must be new and not previously known.
 - **Non-Obviousness:** Cannot be obvious to a person with ordinary skill in the relevant field.
 - Must convince the patent office of its validity.
4. **Enforcement:** Patent holders **must actively oppose all infringement** or risk losing their patent rights.
5. **Software Patents:**
 - Recognized since **1981** in the US.
 - Algorithms **can** be patented if they meet novelty and non-obviousness criteria and are tied to a process or machine.
 - **Real-world Example:** Amazon's "1-Click" purchase patent (though controversial and later expired/invalidated in some regions).
 - 🧠 **Mnemonic:** Patent protects **P**ractical **P**rocesses and inventions.

C. Trade Secrets

1. **Definition:** Information that provides a **competitive advantage** and is kept confidential.
2. **Requirements:** Must be actively **guarded as a secret**. Legal protection is lost if secrecy is not maintained.
3. **Protection Scope:**
 - Protects against **improper acquisition** (e.g., theft, espionage) and use.
 - Does **not** protect against:
 - **Independent discovery** by others.

- **Reverse engineering.**

4. **Software Protection:**

- Can protect **secret algorithms** or methods within software.
- **Cannot** prevent software **piracy** (unauthorized copying).
- **Challenge:** Software is often susceptible to reverse engineering.
- **Real-world Example:** The formula for Coca-Cola. Google's search algorithm details.

D. Comparison Table (Slide 6)

	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

- **Summary:**
 - Copyright = Expression (automatic, long duration, protects against copying).
 - Patent = Invention/Process (requires application/novelty, shorter duration, protects against making/using/selling).
 - Trade Secret = Confidential Info (requires secrecy, potentially indefinite duration, protects against misappropriation).

✦ **Section II Key Takeaways:**

- Copyright, patent, and trade secret offer different types of protection for software and data.
- Copyright protects the code's expression, patents protect novel processes/algorithms, and trade secrets protect confidential information giving a competitive edge.
- Understanding the scope, requirements, and limitations of each is crucial for developers and businesses.

- Fair use allows limited use of copyrighted material. Reverse engineering is generally permissible for trade secrets.
-

III. Special Characteristics of Information

Information possesses unique qualities that differentiate it from tangible assets and influence its legal treatment.

1. **Value:** Information can be highly valuable.
 2. **Non-Depletable:** Using information does not consume it.
 3. **Replicable:** Can be copied easily and perfectly (or near-perfectly).
 4. **Minimal Marginal Cost:** The cost of producing one additional copy is often very low.
 5. **Time-Dependent Value:** Information's relevance and value can decay quickly (e.g., news, stock prices).
 6. **Intangible Transfer:** Often transferred electronically or conceptually without physical exchange.
- **Implication:** These characteristics challenge traditional legal concepts based on physical property.
 - **Connection:** Economics (marginal cost, non-rivalrous goods), Information Theory.
 - **Thought Question:** How should legal frameworks evolve to better address the unique nature of digital information assets?
-

✦ Section III Key Takeaways:

- Information's non-depletable, easily replicable, and low marginal cost nature distinguishes it from physical goods.
 - These characteristics complicate legal protection and ownership concepts.
-

IV. Rights of Employees and Employers

The relationship between employees and employers involves specific considerations regarding intellectual property created during employment.

1. **Ownership of Patents:**

- Generally, the **employer owns the patent** if inventing is part of the employee's job description or if company resources were significantly used.
- Even if patented by the employee, the employer might retain **"shop rights"** (a non-exclusive license to use) if their resources contributed.

2. **Ownership of Copyrights:**

- Similar principles to patents, often governed by **"work for hire"** doctrine in the US. If created within the scope of employment, the employer is typically considered the author and owner.

3. **Licenses:**

- A programmer (owner) can grant a company a **license** (permission) to use a program under specific terms (duration, users, systems, etc.) in exchange for a fee.

4. **Trade Secret Protection:**

- Companies own their **business-confidential data** and processes developed internally.
- Employees typically have a duty (often contractual via NDAs) to protect employer trade secrets.

- **Connection:** Contract Law, Labor Law, Intellectual Property Law.
 - **Real-world Example:** Disputes over ownership of code written by an employee using company equipment but outside of core job duties.
 - **► Further Research:** Investigate the specifics of "work for hire" agreements and "shop rights" in your jurisdiction.
 - **Thought Question:** What are the ethical considerations for employees using skills/knowledge gained at one company when moving to a competitor?
-

✦ **Section IV Key Takeaways:**

- Ownership of IP created during employment usually favors the employer, especially if it's within job duties or uses company resources.
 - Employment contracts (NDAs, IP agreements) are critical in defining these rights.
 - Licensing allows controlled use of IP without transferring ownership.
-

V. Responsible Vulnerability Disclosure

A structured process for reporting software flaws aims to balance security improvement with minimizing harm.

- **Proposed Model for Reporting:**
 1. **Confidential Acknowledgement:** Vendor acknowledges report privately to the reporter.
 2. **Confidential Verification:** Vendor confirms (or disputes) the vulnerability privately.
 3. **User Notification:** Vendor informs users of the vulnerability and countermeasures within **30 days** (or requests extension).
 4. **Quiet Period (Optional):** Vendor may request a 30-day quiet period after user notification for patching.
 5. **Public Disclosure:** Vendor and reporter agree on a public release date after the quiet period.
 6. **Credit:** Vendor credits the reporter.
 7. **Coordinator Involvement:** If the vendor is unresponsive, the reporter may work with a third-party coordinator (e.g., CERT/CC) for disclosure.
 - **Connection:** Cybersecurity Risk Management, Public Relations, Ethics.
 - **Real-world Example:** Google's Project Zero often follows a strict disclosure timeline (e.g., 90 days).
 - **Thought Question:** What are the potential negative consequences if vendors *don't* follow a responsible disclosure process? What if researchers disclose immediately without vendor notification?
-

✦ Section V Key Takeaways:

- Responsible vulnerability disclosure is a process to manage the discovery and remediation of software flaws safely.
 - It involves confidential communication, timely vendor response, user notification, and coordinated public release.
-

VI. Computer Crime: Legal Aspects

Applying traditional legal concepts to the digital realm presents unique challenges.

A. Foundational Legal Concepts

1. **Rules of Property:** Laws generally recognize **data and computer services as property** that can be owned, stolen, or damaged.
2. **Rules of Evidence:**
 - **Authenticity Challenge:** Proving digital evidence hasn't been tampered with is difficult.
 - **Chain of Custody:** Crucial for admissibility. Meticulously tracking who handled the evidence and when.
3. **Threats to Integrity & Confidentiality:** Laws increasingly recognize unauthorized access, data modification, and privacy breaches as specific crimes.
4. **Value of Data:** Legally, digital data's value is often determined by what a willing buyer would pay (market value).

B. Challenges in Prosecution

Computer crime prosecution faces several hurdles:

1. **Lack of Understanding:** Courts, lawyers, law enforcement, and juries may lack technical expertise.
 2. **Lack of Physical Evidence:** Crimes are often intangible.
 3. **Lack of Political Impact:** Harm may be diffuse or financial, not directly physical (though this is changing).
 4. **Complexity:** Cases often involve intricate technical details and cross-jurisdictional issues.
 5. **Age of Defendants:** Offenders are often juveniles, leading to different legal handling.
 6. **Victim Reluctance:** Organizations (e.g., banks) may avoid prosecution due to fear of reputational damage and loss of customer trust.
- **Connection:** Criminal Law, Digital Forensics, Procedural Law.
 - **Thought Question:** How can law enforcement and judicial systems improve their capacity to handle complex cybercrime cases effectively?

✦ Section VI Key Takeaways:

- Legal systems have adapted to treat data as property and breaches as crimes, but challenges remain.
- Proving digital evidence authenticity (chain of custody) is critical but difficult.
- Prosecuting cybercrime is hampered by technical complexity, lack of understanding, jurisdictional issues, and victim reluctance.

VII. Key Computer Security Statutes

Various laws address specific aspects of computer crime, privacy, and security. (Note: This list is based on the 2015 text; newer laws like GDPR/CCPA are also highly relevant now).

A. United States Laws

1. **Computer Fraud and Abuse Act (CFAA)**: Cornerstone federal anti-hacking law. Prohibits unauthorized access, computer fraud, password trafficking, damaging transmissions.
2. **Economic Espionage Act**: Criminalizes theft of trade secrets, including via computer, especially for foreign benefit.
3. **Freedom of Information Act (FOIA)**: Provides public access to information held by the federal executive branch (with exceptions).
4. **Privacy Act of 1974**: Governs collection, maintenance, use, and dissemination of personally identifiable information (PII) by federal agencies.
5. **Electronic Communications Privacy Act (ECPA)**: Protects wire, oral, and electronic communications while in transit and storage. Sets rules for wiretaps.
6. **Gramm-Leach-Bliley Act (GLBA)**: Requires financial institutions to protect customer NPI (Nonpublic Personal Information) and disclose privacy practices.
7. **Health Insurance Portability and Accountability Act (HIPAA)**: Mandates protection and privacy of Protected Health Information (PHI).
8. **USA PATRIOT Act**: (Post-9/11) Expanded surveillance powers, including easier wiretaps for foreign intelligence; increased penalties for damaging computer systems.
9. **CAN-SPAM Act**: Regulates commercial email; requires opt-outs, prohibits deceptive headers/subjects.
10. **California Breach Notification Law (SB 1386/Civ Code 1798.82)**: First state law requiring notification to residents if their PII is compromised in a data breach. (Many states followed).

B. International / Regional Agreements

1. **Council of Europe Convention on Cybercrime (Budapest Convention)**: International treaty harmonizing cybercrime laws and facilitating international cooperation in investigations.
2. **EU Data Protection Directive (Superseded by GDPR)**: Established baseline privacy rights and data controller responsibilities across EU member states. (GDPR - General

Data Protection Regulation is the current, stricter standard).

- 🧠 **Mnemonic Focus:** Key Acts: **CFAA** (Hacking), **ECPA** (Wiretap/Privacy), **GLBA** (Finance Privacy), **HIPAA** (Health Privacy), **GDPR/CCPA** (Modern Privacy Regs - *though not on slides*).
- 📖 **Additional Resources:** Look up summaries of GDPR (General Data Protection Regulation) and CCPA (California Consumer Privacy Act) / CPRA (California Privacy Rights Act) as they are major recent developments.
- 📄 **Potential Exam Question:** Select two laws (e.g., HIPAA and GLBA) and explain their primary security/privacy requirements and the sector they primarily apply to.
- 🚩 **Flag:** Legislation changes rapidly. Always verify the current status and amendments to these laws.

📌 Section VII Key Takeaways:

- A complex web of federal, state, and international laws governs computer security, crime, and data privacy.
- Key US laws include CFAA, ECPA, HIPAA, and GLBA, each addressing specific areas.
- International agreements like the Budapest Convention aim for cross-border cooperation. Privacy regulations (like GDPR) have global impact.

VIII. Ethics in Computing

Beyond legal requirements, ethical principles guide behavior in computing.

A. Law vs. Ethics (Slide 15)

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


- **Summary:** Laws are formal rules with legal consequences; ethics are moral principles guiding right/wrong conduct, often without formal enforcement but with social/personal consequences. An action can be legal but unethical, or illegal but potentially perceived as ethical in some contexts (e.g., civil disobedience).

B. Framework for Ethical Analysis (Slide 16)

A structured approach to evaluating ethical dilemmas:

1. **Understand the Situation:** Gather all relevant facts.
2. **Know Ethical Theories:** Be aware of different ethical reasoning approaches (see below).
3. **List Ethical Principles Involved:** Identify conflicting values (e.g., privacy vs. security, honesty vs. loyalty).
4. **Determine Principle Priority:** Decide which principles are more significant in this context.
5. **Make and Defend Choice:** Formulate a decision and justify it based on the ethical reasoning.

C. Bases of Ethical Theories (Slide 17)

- *[Instruction: Insert the diagram/table from Slide 17. This likely shows categories like:]*
 - **Consequence-based (Teleological):** Focuses on outcomes. **Utilitarianism** (greatest good for the greatest number) is a key example.
 - **Rule-based (Deontological):** Focuses on duties, rights, and rules, regardless of outcome. Following universal moral laws (e.g., Kant's Categorical Imperative).
 - **(Potentially Others):** Virtue Ethics (focus on character), Rights-based ethics, etc.
-  **Additional Resource:** Explore resources like the Stanford Encyclopedia of Philosophy or Markkula Center for Applied Ethics (Santa Clara University) for deeper dives into ethical theories.

D. Ethical Scenarios/Case Studies

(Brief summaries and key ethical questions for each)

1. **Situation I (Use of Computer Services - Dave):** Programmer uses company computer off-hours for personal project (minimal impact).
 - **Ethical Qs:** Is unauthorized use of resources ever acceptable if no harm occurs? Does it violate company policy (rule-based)? Is it fair to the employer (rights)?

2. **Situation II (Privacy Rights - Donald/Ethel):** Researcher asks clerk for names/addresses linked to anonymized data previously provided for study.
 - **Ethical Qs:** Does Donald have a duty to protect privacy (rule/rights)? Does the potential benefit of Ethel's research outweigh the privacy intrusion (consequence)? What was the initial agreement for data access?
3. **Situation III (Denial of Service - Charlie/Carol):** Accidental vs. potentially intentional triggering of system flaw causing crashes. Director inspects files, suspends one student (Carol).
 - **Ethical Qs:** Is Carol's action (if intentional) ethical? Was Charlie negligent? Was the Director's inspection of Carol's files justified (privacy vs. system security)? Was the punishment proportionate?
4. **Situation IV (Ownership of Programs - Greg/Cathy):** Programmer develops tools at home, company claims ownership, supervisor (Cathy) later uses them at competitor.
 - **Ethical Qs:** Who truly owns the tools (contract vs. effort)? Was Cathy's initial reluctance ethical? Was taking/using the tools at the new company ethical (theft/misappropriation)? Is Cathy's "public domain" argument valid?
5. **Situation V (Proprietary Resources - Suzie/Luis):** Legitimate owner demonstrates copyrighted/licensed software, friend wants to "try it longer."
 - **Ethical Qs:** Does demonstrating violate the license? Would letting Luis use it longer constitute unauthorized copying/use? What is Suzie's ethical obligation regarding the license terms?
6. **Situation VI (Fraud - Alicia/Ed):** Programmer asked to create a tool bypassing accounting controls.
 - **Ethical Qs:** Does Alicia have an ethical duty to refuse an order that enables potential fraud (professional responsibility)? What are the consequences of creating/not creating the tool? Loyalty to supervisor vs. integrity? Whistleblowing?
7. **Situation VII (Accuracy of Information - Emma/Paul):** Researcher's data doesn't support desired outcome; asks statistician (Paul) to analyze. Data looks bad, Paul notes analyses could make it look better.
 - **Ethical Qs:** What is Paul's ethical obligation regarding truthful representation of data? Should he perform misleading analyses if asked? What are Emma's ethical obligations to the funding source and scientific integrity?
8. **Situation VIII (Ethics of Hacking/Cracking - Goli):** Consultant attacks products, probes systems (offers fixes), and disrupts websites of disliked businesses.
 - **Ethical Qs:** Is unsolicited vulnerability testing ethical? Is offering services after finding flaws ethical (or extortionate)? Is attacking/disrupting systems ever ethical, even for perceived "good" or trivial reasons?

- **Connection:** Professional Codes of Ethics (e.g., ACM Code of Ethics and Professional Conduct).
-

✦ Section VIII Key Takeaways:

- Ethics provides a framework for navigating moral dilemmas in computing where laws may be insufficient or ambiguous.
 - Analyzing situations requires understanding facts, applying ethical theories (consequence-based, rule-based), identifying conflicting principles, and justifying choices.
 - Common ethical issues involve privacy, property rights, accuracy, honesty, confidentiality, and responsible use of power/access.
-

IX. Summary (Slide 26)

- Legal tools like **copyrights, patents, and trade secrets** offer distinct protections for software IP.
 - Legal and contractual details shape **relationships** between employees, employers, vendors, and customers regarding software.
 - Numerous **statutes** define computer crimes and mandate security/privacy practices, but enforcement faces challenges.
 - **Ethical considerations** involve personal and philosophical dimensions, often requiring nuanced judgment beyond strict legal compliance.
-

Glossary of Key Terms

- **Copyright:** Legal right protecting the *expression* of an idea (e.g., source code).
- **Patent:** Legal right protecting an *invention* or process (e.g., a novel algorithm).
- **Trade Secret:** Confidential information providing a competitive edge, protected by maintaining secrecy.
- **Fair Use:** Legal doctrine permitting limited use of copyrighted material without permission for specific purposes (e.g., criticism, education).
- **Novelty:** A key requirement for patentability; the invention must be new.

- **Chain of Custody:** The documented chronological history of evidence handling, crucial for admissibility in court.
 - **Responsible Vulnerability Disclosure:** A process for reporting security flaws to vendors in a way that minimizes harm.
 - **CFAA (Computer Fraud and Abuse Act):** Primary US federal law against hacking and computer fraud.
 - **ECPA (Electronic Communications Privacy Act):** US law protecting electronic communications from wiretapping/interception.
 - **GLBA (Gramm-Leach-Bliley Act):** US law requiring financial institutions to protect customer information privacy.
 - **HIPAA (Health Insurance Portability and Accountability Act):** US law protecting the privacy and security of health information.
 - **Work For Hire:** Legal doctrine where work created by an employee within the scope of employment is owned by the employer.
 - **License:** Permission granted by the owner to use intellectual property under specific terms.
 - **Ethics:** Moral principles governing behavior, distinct from but related to law.
-

Mind Map / Concept Diagram Structure

- **Central Topic:** Legal & Ethical Issues in Computing
 - **Branch 1: Intellectual Property Protection**
 - Sub-branch: Copyright (Expression, Fair Use, Code)
 - Sub-branch: Patent (Invention, Novelty, Algorithms)
 - Sub-branch: Trade Secret (Confidentiality, Competitive Edge, Reverse Engineering)
 - Sub-branch: Comparison (Table/Key Differences)
 - **Branch 2: Information Characteristics** (Non-depletable, Replicable, Low MC, Time Value)
 - **Branch 3: Employer/Employee Rights** (Patents, Copyrights/Work-for-Hire, Licenses, Trade Secrets)
 - **Branch 4: Vulnerability Disclosure** (Process Steps, Vendor/Reporter Roles, Coordination)
 - **Branch 5: Computer Crime Law**
 - Sub-branch: Legal Concepts (Data as Property, Evidence/Chain of Custody)

- Sub-branch: Prosecution Challenges (Complexity, Evidence, Understanding)
 - **Branch 6: Key Statutes**
 - Sub-branch: US (CFAA, ECPA, GLBA, HIPAA, etc.)
 - Sub-branch: International (Budapest Convention, EU Regs)
 - **Branch 7: Ethics**
 - Sub-branch: Law vs. Ethics
 - Sub-branch: Ethical Analysis Framework
 - Sub-branch: Ethical Theories (Consequentialism, Deontology)
 - Sub-branch: Case Studies (Link to each scenario)
-

Made by Yashank