CS 230: Ethical Issues in Computing

- Roster and passwords
- Our `pub` directory:

  `onyx:~jbuffenb/classes/230/pub`
- Our lecture slides:

  `pub/slides/slides.pdf`
- Review syllabus

  `http://cs.boisestate.edu/~buff`

  `pub/syllabus/syllabus.pdf`
- Introduction

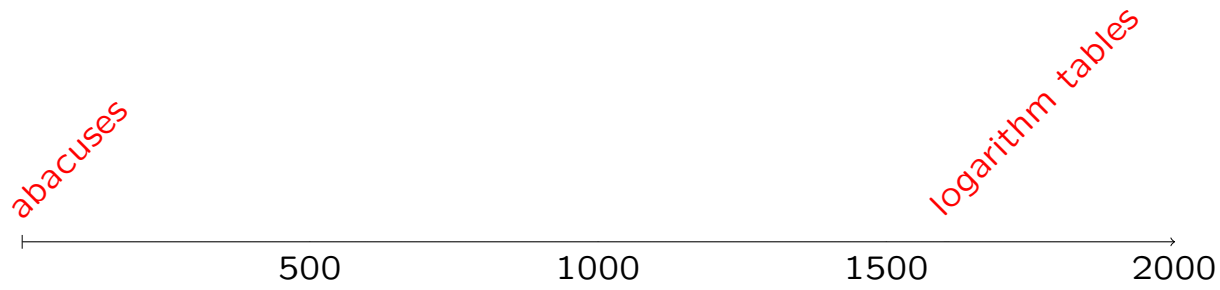
Chapter 1: Catalysts for Change

- We will be discussing a period of time called the *information age*, which is defined by low-cost computers and high-speed communication networks.
- In 1950, there were only a handful of electronic digital computers. Indeed, a famous (mis)quote of IBM's Thomas J. Watson was: "I think there is a world market for maybe five computers."
- In 1990, email was popular primarily in the academic community.
- Today, nearly a billion people use email.
- Technology affects our lives, both physically and in the way we perceive the world. It can improve our lives, but it can cause problems. We may not be able to stop technological advances, but we can influence the way and rate at which we adopt it.

Introduction

- We will define terms in later chapters, but here is a look ahead.
- Every society has rules of conduct describing appropriate behavior, called *morality*.
- Each society has its own morality. Different societies can disagree, strongly and emotionally, about what is moral behavior.
- On the other hand, we can be *philosophical*: meeting trouble with level-headed detachment.
- *Ethics* is the philosophical study of morality.
- In this course, we focus on parts of ethics relevant to societal changes occurring in the information age.
- But first, we will study some relevant history.

Early calculators and computers (1 of 4)



- Over 2000 years ago, the abacus was used to perform simple computations, as were simple mathematical tables.
- In the early 1600s, tables of logarithms became available, allowing multiplication to be done by addition.
- Currency-conversion tables were also used. Of course, these tables were produced manually.

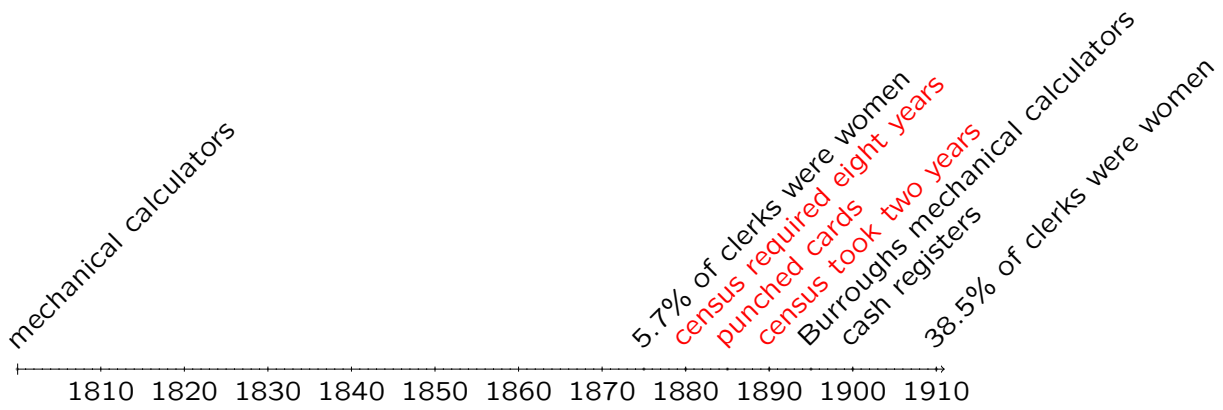
Early calculators and computers (2 of 4)

- In the 1800s, improved machine tools were able to fabricate mechanical calculators, like the Arithometer. In 1856, these calculators could automatically typeset mathematical tables.
- In the late 1800s and early 1900s, mechanical calculators made by Burroughs became very popular.
- Burroughs claimed that a calculator user was six times more productive than a clerk performing manual computation.

Early calculators and computers (3 of 4)

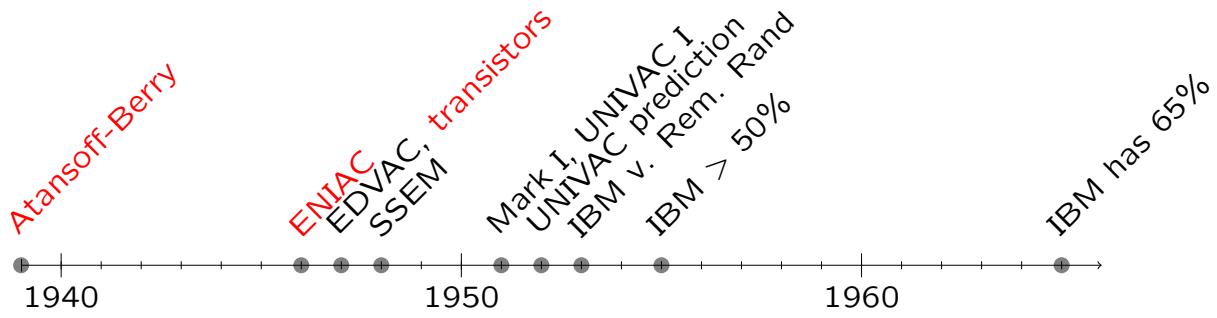
- They also changed the office demographic. In 1880, 5.7% of clerks were women. In 1910, this had changed to 38.5%.
- In the early 1900s, cash registers became popular. Aside from automatic accounting, they prevented clerks from embezzling their employers.

Early calculators and computers (4 of 4)



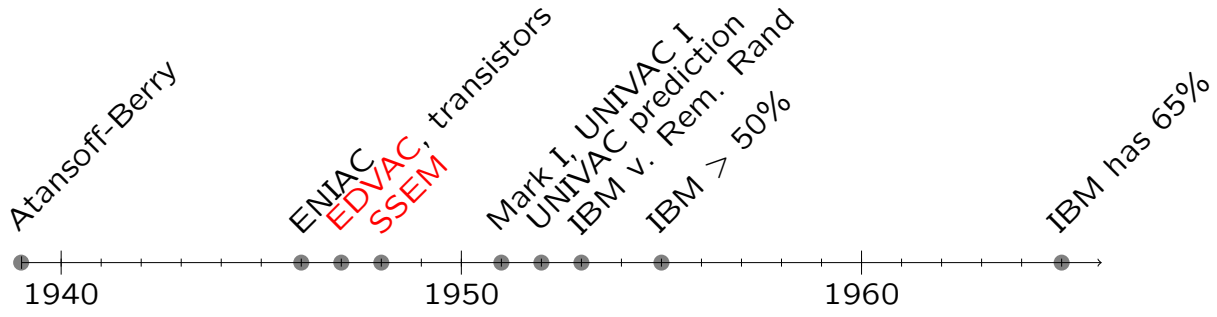
- In the late 1880s, the U.S. Census Bureau used Hollerith's punched cards to record and tabulate data.
- The 1880 census required eight years; the 1890 census was done in two years.
- These cards could be mechanically analyzed, sorted, and reproduced. Intermediate results could also be mechanically punched onto cards. In fact, the steps of the computational process (i.e., the program) could also be on cards. International Business Machines (IBM) and Remington Rand were vendors of such data-processing systems.

Later computers (1 of 4)



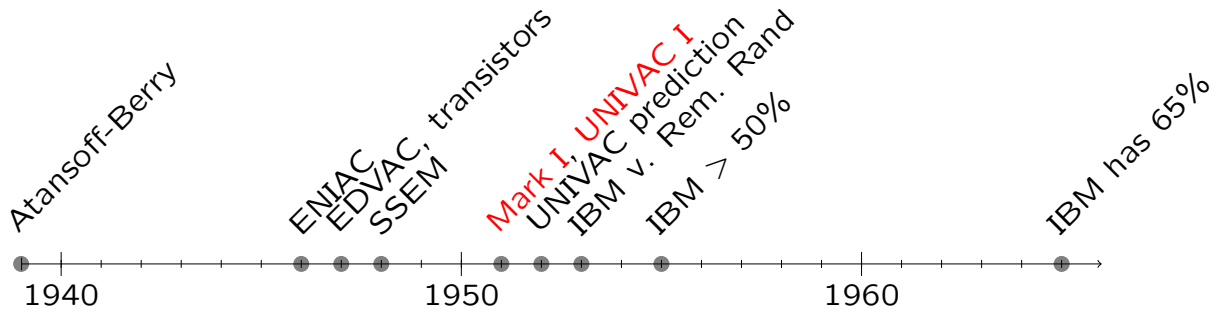
- During and following World War II, several digital computers were developed.
- In 1939, the Atansoff-Berry computer was built with vacuum tubes. Various transistors would be developed in 1947–1954. It was not programmable. It solves systems of linear equations.
- In 1946, the programmable Electronic Numerical Integrator and Computer (ENIAC) was built. It was 2,400 times faster than a calculator. Its program comprised wires plugged into an external plugboard, rather than instructions in memory. It was intended to compute missile-trajectory tables.

Later computers (2 of 4)



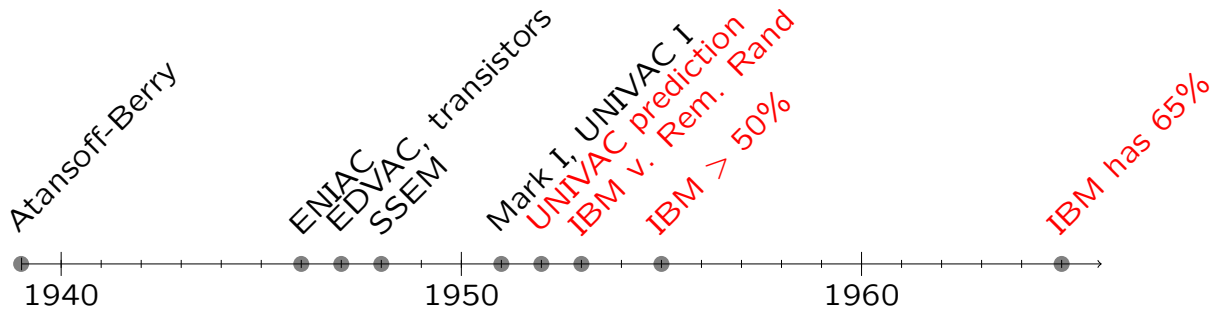
- Soon after, the Electronic Discrete Variable Automatic Computer (EDVAC) was built. Its program was stored in memory, along with the program's data.
- In 1948, the Small-Scale Experimental Machine (SSEM) was built, in Britain, with a cathode ray tube (CRT) as a storage device for programs and data. Previously, CRTs were used in radar systems. Since the ENIAC and EDVAC used punched cards, the SSEM was the first fully electronic computer.

Later computers (3 of 4)



- In 1951, the Ferranti Mark I, the first commercial computer was developed, in Britain by the SSEM group. Nine were delivered, between 1951 and 1957.
- In 1950, the ENIAC group was rescued from bankruptcy by Remington Rand, who delivered the UNIVAC I to the U.S. Census Bureau, in 1951. In all, 46 UNIVACs were sold.
- Notice how much progress and innovation was occurring during this brief period. Although people tried to patent these inventions, enforcement was confusing and difficult.

Later computers (4 of 4)

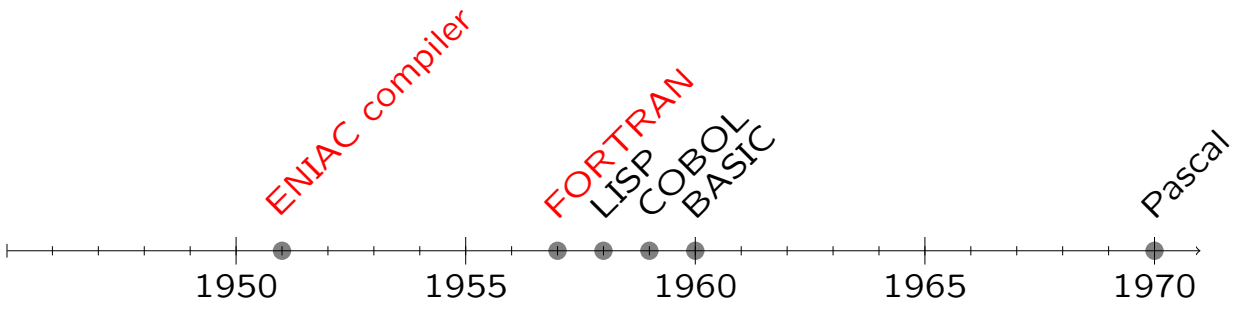


- A UNIVAC was used by Columbia Broadcasting System (CBS) to predict the outcome of the 1952 Presidential election. Political experts did not believe part of the prediction, so the "buggy" program was changed to conform to their opinion. The original program's prediction proved correct.
- In 1953, IBM began competing with Remington Rand. By 1955, IBM held more than half of the market. By the mid-1960s, IBM held 65% of sales, compared to 12% for now-named Sperry Rand.

Programming languages (1 of 4)

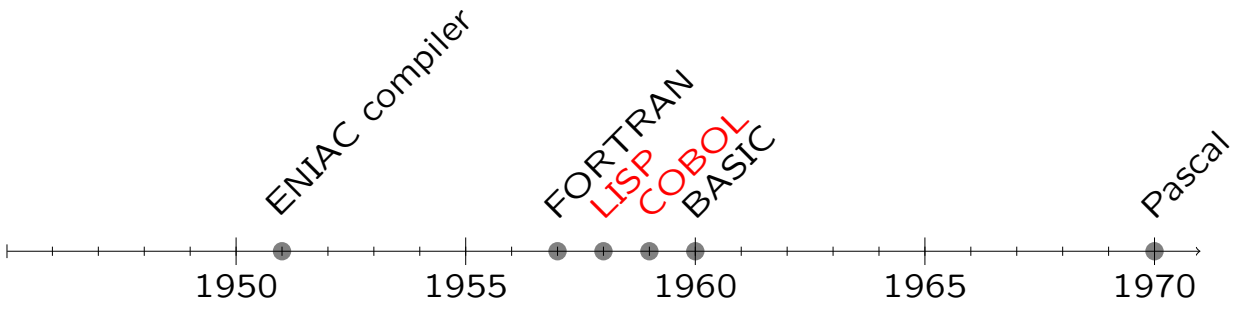
- Fundamentally, an electronic digital computer executes a *machine-language* program, a sequence of *machine instructions*, each of which is a binary number.
- An improvement is for a programmer to write an *assembly-language* program, a sequence of *assembly-language* instructions, each of which is a mnemonic opcode for a machine-language opcode (e.g., `ld`) followed by symbolic operands (e.g., `r0` or `total`).
- A program called an *assembler* translates an assembly-language program into a machine-language program. By definition, instruction translation is one-for-one. After some hardware evolution, the ENIAC had an assembler.

Programming languages (2 of 4)



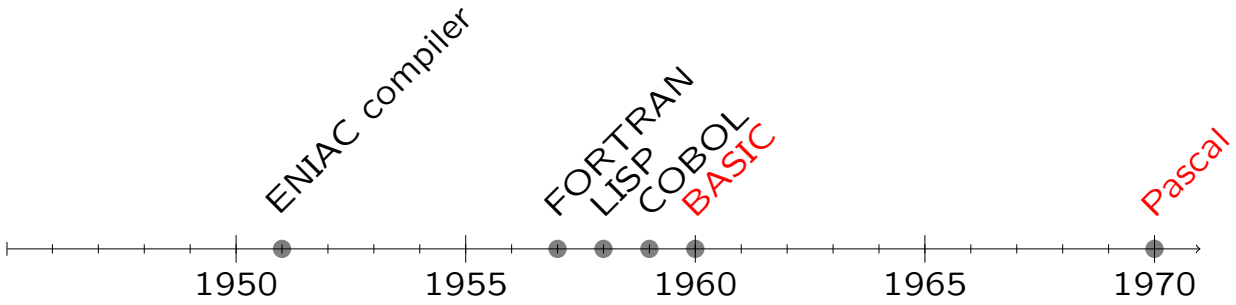
- In 1951, a higher-level translator, a *compiler*, was developed for the ENIAC. An abstract sort/merge specification would compile to a machine-language program. Also, a *linker*, which could combine machine-language modules, was developed.
- In 1957, IBM (John Backus) developed the Mathematical Formula Translating System (FORTRAN), which is still very popular.

Programming languages (3 of 4)



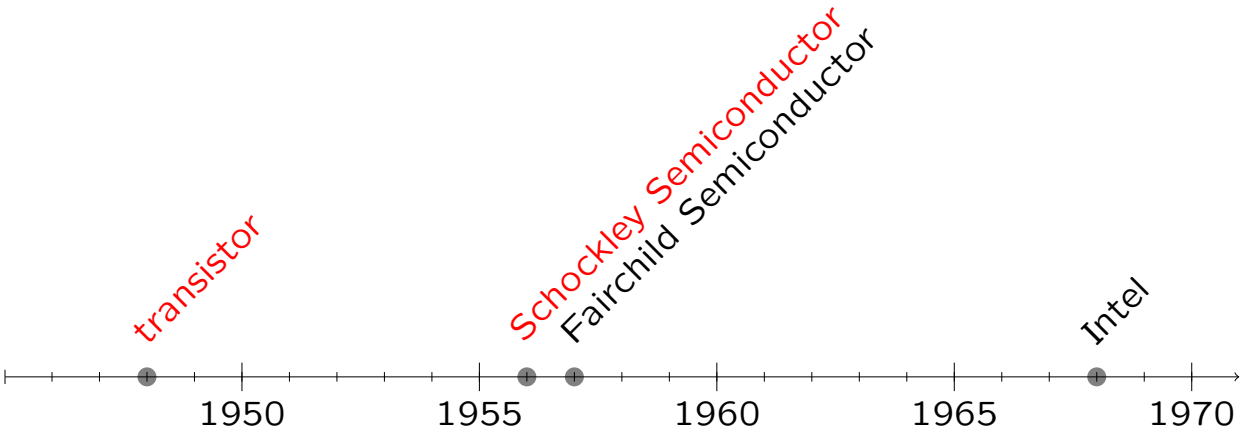
- In 1958, the Massachusetts Institute of Technology (MIT) (John McCarthy) developed the List Processing language (LISP), for symbolic computation. It became popular in the artificial-intelligence (AI) community. It is still popular.
- In 1959, a committee organized by the U.S. Department of Defense (Grace Hopper) developed the Common Business-Oriented Language (COBOL), which is still around.

Programming languages (4 of 4)



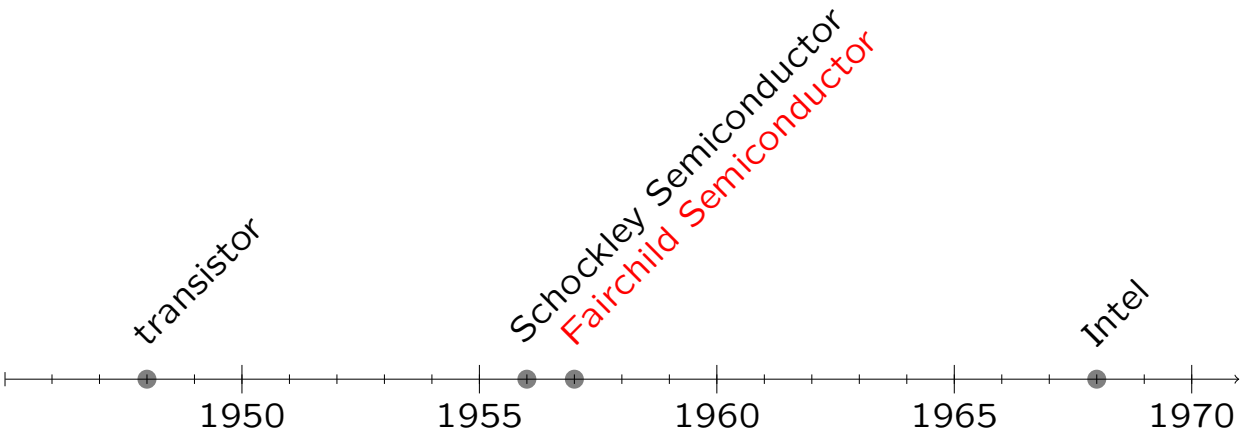
- In 1960, a group at Dartmouth (John Kemeny and Thomas Kurtz) developed the Beginner's All-Purpose Symbolic Instruction Code (BASIC), which was used as a teaching language until supplanted by Pascal in the 1980s.
- In 1970, ETH Zurich (Niklaus Wirth) developed Pascal. Pascal is a simple language, based on Algol. It is representative of imperative block-structured languages (e.g., C), and their object-oriented successors (e.g., C++ and Java).

Transistor and integrated circuit (1 of 3)



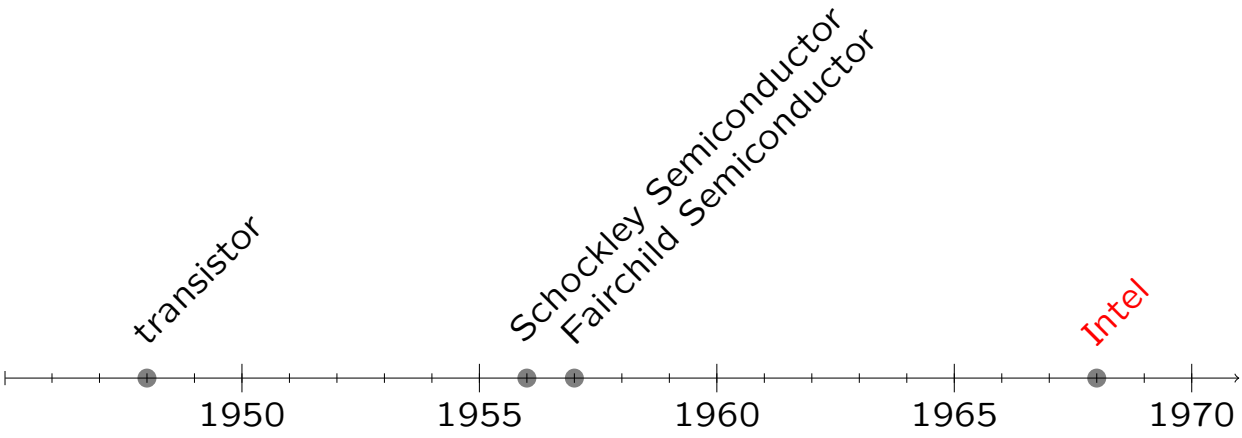
- In 1948, Bell Labs (Bill Schockley) announced the invention of the transistor.
- In 1956, Schockley formed Schockley Semiconductor, in Palo Alto, California.
- In 1957, eight of his best employees, including Gordon Moore and Robert Noyce, left and formed Fairchild Semiconductor.
- Reports say Schockley went kind of kooky.

Transistor and integrated circuit (2 of 3)



- Independently, Fairchild Semiconductor and Texas Instruments developed the *integrated circuit* (IC) (aka, chip), a single semiconductor device containing transistors, resistors, and capacitors.
- During World War II, Sherman Fairchild sold bombsights. At one time, he owned most of IBM's stock.
- Later, NASA was buying 90% of the chips Fairchild Semiconductor built.

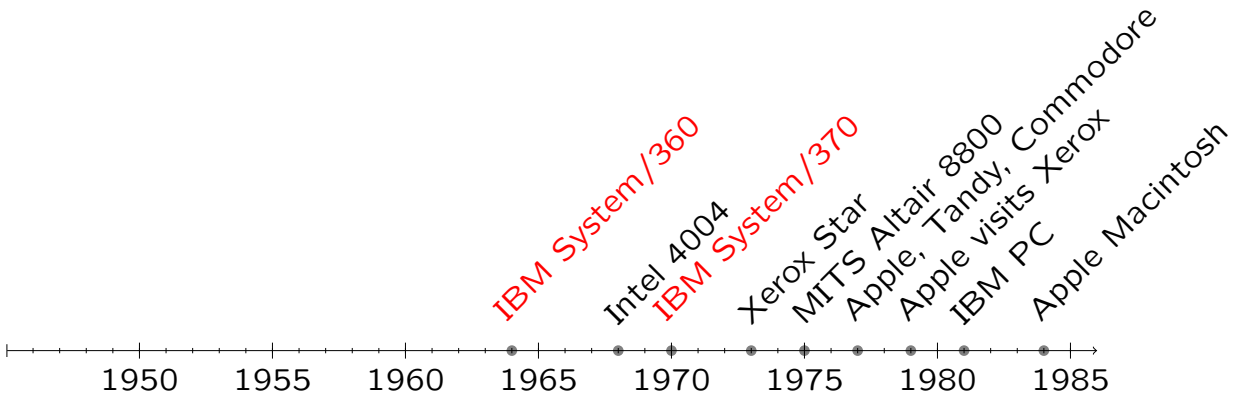
Transistor and integrated circuit (3 of 3)



- In 1968, Moore and Noyce formed Intel, which developed memory and processor chips. You may have heard of them.
- Intel was one of many so called Fairchildren:

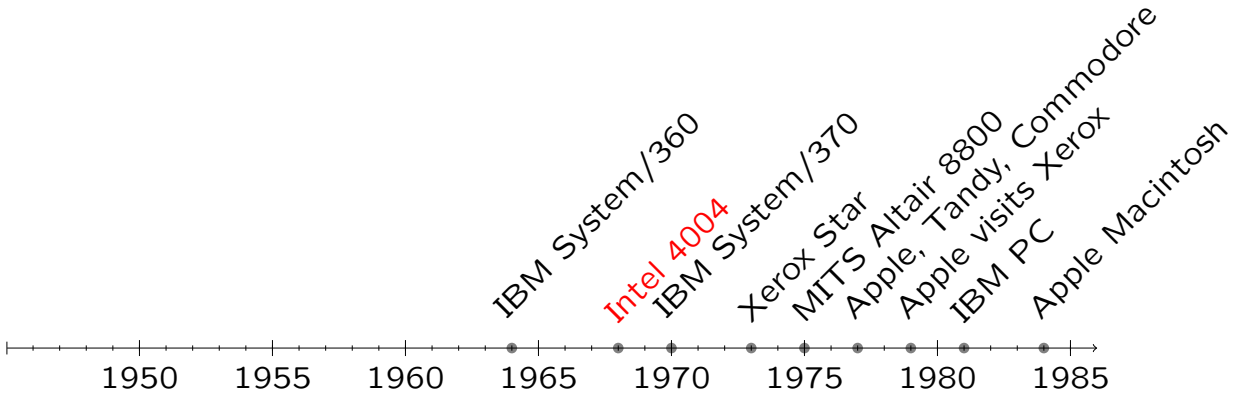
  pub/ch1/fairkid.pdf

Commercial computers (1 of 8)



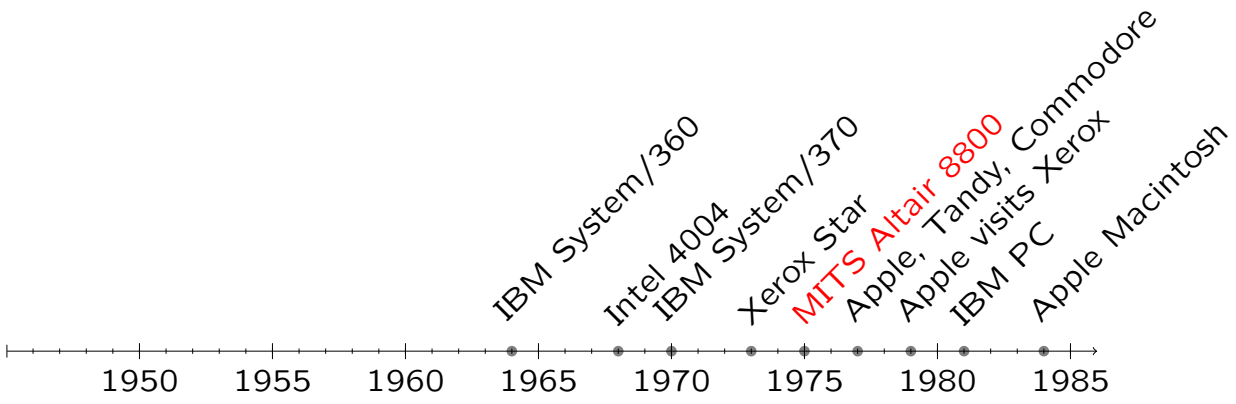
- In 1964, IBM announced a family of 19 compatible mainframe computers.
- In 1970, it was succeeded by the IBM System/370 family.
- Both families were very successful. A customer could only lease a computer. The operating system was included at no extra cost.

Commercial computers (2 of 8)



- In 1968, Moore and Noyce left Fairchild to form Intel.
- Intel was asked to develop a calculator chip, but an engineer (Ted Hoff), felt that a mere 12 chips were too complex to build below budget, so he suggested a general-purpose programmable chip: a *microprocessor*.
- Federico Faggin led development of the Intel 4004, a $\frac{1}{8}'' \times \frac{1}{6}''$ chip, with the same computing power as the ENIAC, which occupied 3,000 cubic feet (about 85 refrigerators).

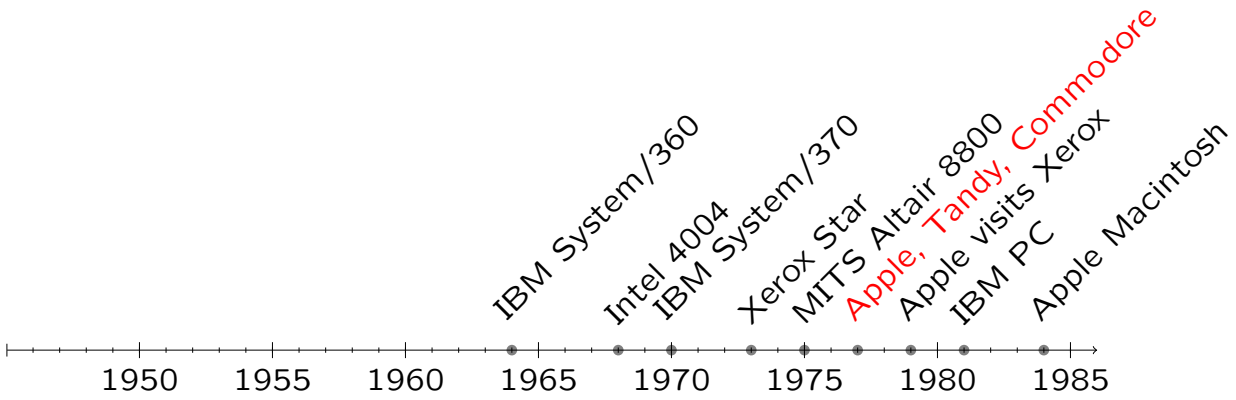
Commercial computers (3 of 8)



- In 1975, the MITS Altair 8800 was available, for $400 (kit) or $500 (assembled). It was a *microcomputer*: a microprocessor-based computer.
- Microsoft (Paul Allen and Bill Gates) offered a BASIC translator for it, for $500.
- However, the translator's source code was widely distributed (illegally) for free. Gates wrote:

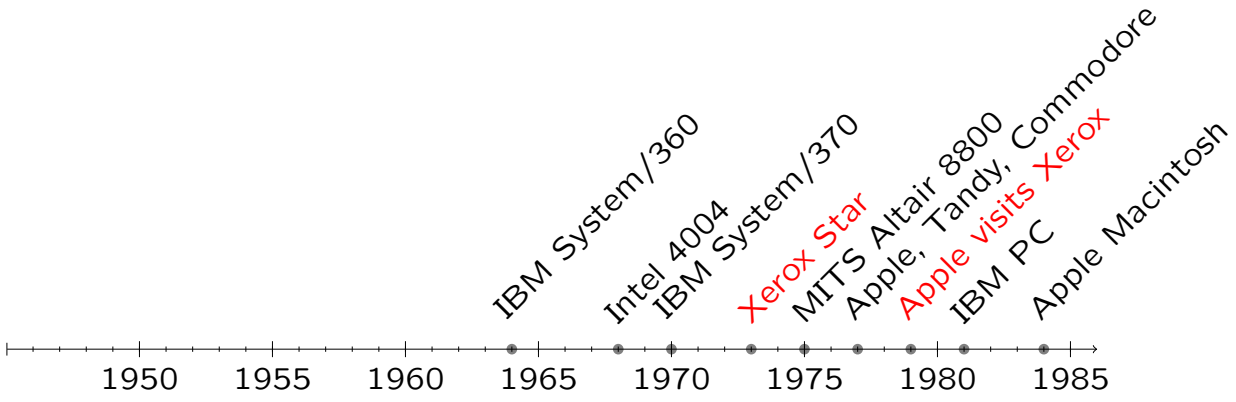
  `pub/ch1/gates`

Commercial computers (4 of 8)



- By the end of the 1970s, many companies, including Apple and Tandy (i.e., Radio Shack), and Commodore (Paul Allen's "1977 Trinity"), were selling personal computers.
- Apple sold 200 Apple I computers and over 5 million Apple II computers.

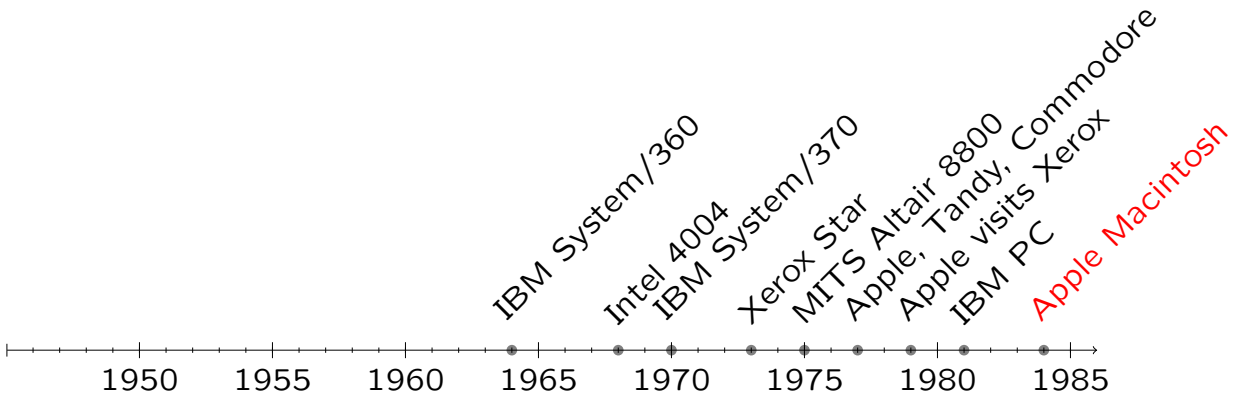
Commercial computers (5 of 8)



- In 1973, Xerox's Palo Alto Research Center (PARC) introduced the Star, which greatly influenced future developments at Apple, Microsoft, and Sun Microsystems.
- In 1979, Xerox was allowed to buy 10% of Apple's pre-IPO stock in exchange for engineer visits and an understanding that Apple would create a graphical user interface (GUI) product. This is described in:

  pub/ch1/ftf.jpg

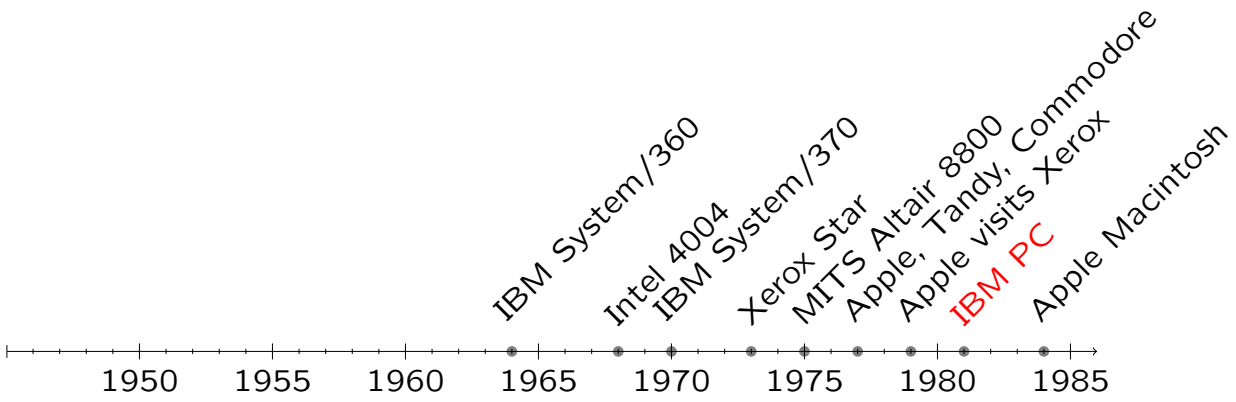
Commercial computers (6 of 8)



- In 1984, Apple's Macintosh was the first successful commercial product with a GUI, which was heavily inspired by PARC's work.
- In the first year, 300,000 were sold.
- Later, in a lawsuit, Apple accused Microsoft of violating its copyright by appropriating the use of the "look and feel" of the Macintosh GUI. Apple lost.
- Xerox sued Apple on the same grounds, but the lawsuit was dismissed because the statute of limitations had expired.
- Ironic quotes:

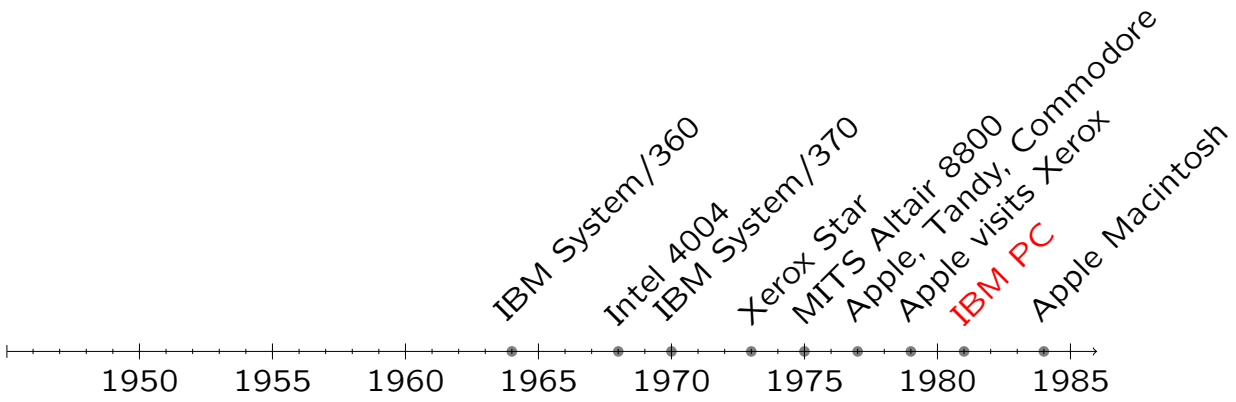
  pub/ch1/laf

Commercial computers (7 of 8)



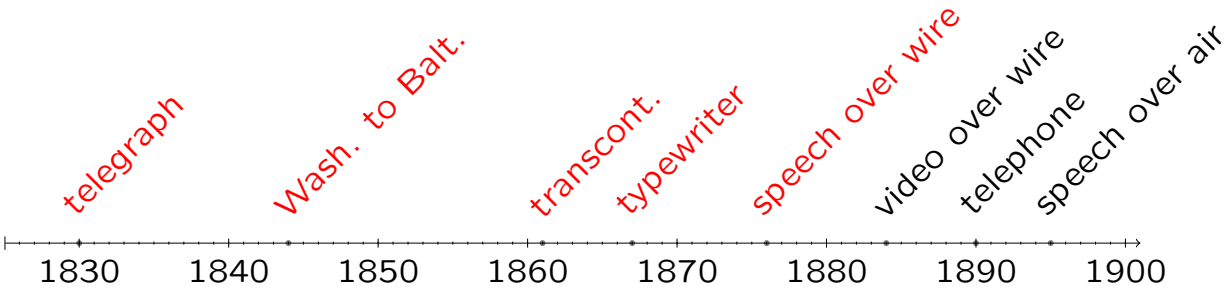
- In 1981, IBM released the IBM PC. Development time was limited to just one year.
- While Apple's architecture was proprietary, IBM's architecture was open. This allowed IBM-clone PCs to proliferate.
- IBM compatible PCs acquired 80% of the PC market.

Commercial computers (8 of 8)



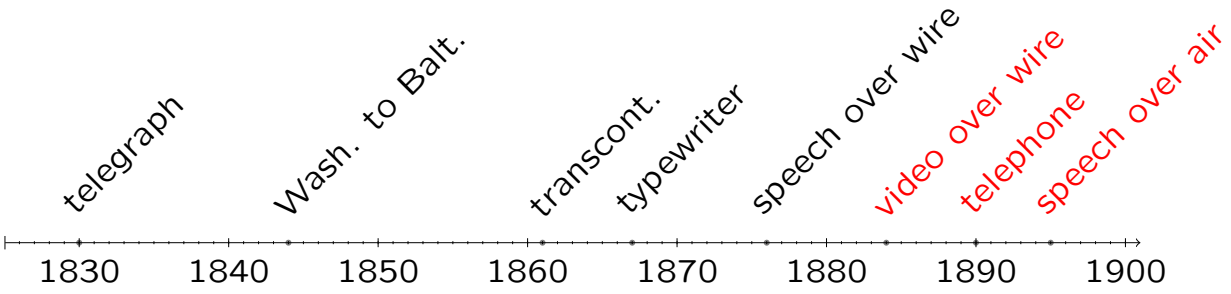
- Microsoft provided IBM with an operating system, for its PC, almost for free. However, IBM gave Microsoft the right to collect royalties from companies producing clones.
- Actually, Microsoft bought QDOS from a guy in Seattle, for $50,000, named it MS-DOS, so that IBM could rename it to PC DOS.

Early communication (1 of 3)



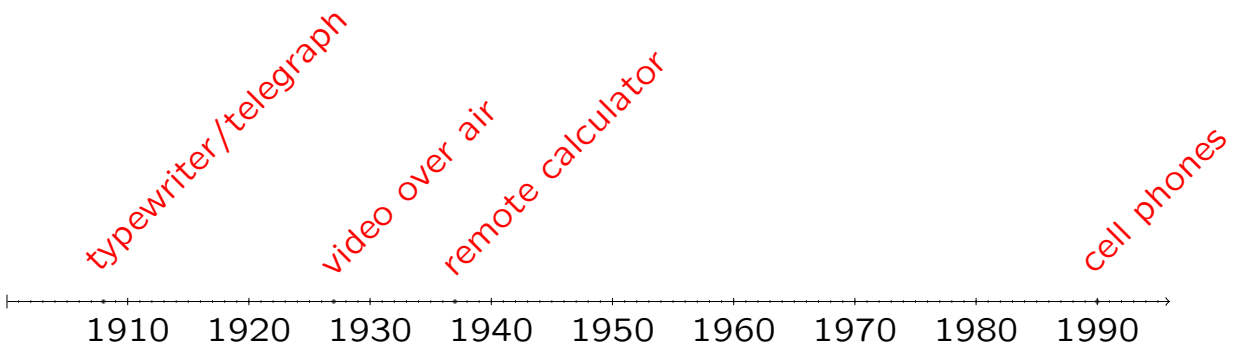
- In 1830, an electric telegraph was demonstrated.
- In 1844, a telegraph was strung from Washington to Baltimore.
- In 1861, a transcontinental telegraph was completed.
- In 1867, the first typewriter was patented.
- In 1877, the U.S. had over 200,000 miles of telegraph.
- In 1876, Alexander Graham Bell and Thomas A. Watson transmitted speech electrically. They patented and commercialized their invention.

Early communication (2 of 3)



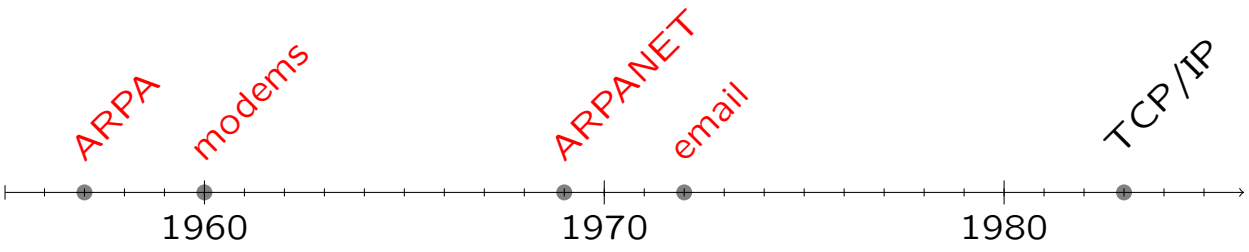
- In 1884, video was transmitted, electromechanically, over a wire.
- In 1885, electromagnetic waves were generated.
- In the 1890s, after the patent expired, the number of residential telephones increased rapidly. Privacy and intrusion complaints began.
- In 1895, radio signals were transmitted over the air.

Early communication (3 of 3)



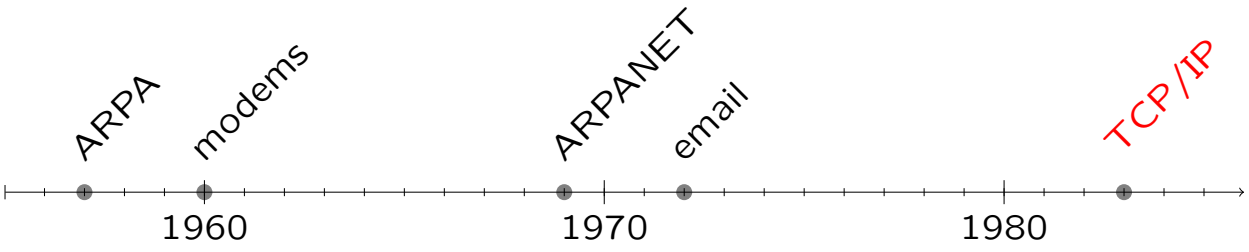
- In 1908, a typewriter was modified to transmit a message over a telegraph line.
- In 1927, video was transmitted, electronically, over the air.
- In 1937, an electromechanical adder was connected to a teletype machine, forming the first remotely operated calculator.
- In the 1990s, cell phones became popular. Now, they outnumber wired telephones.

Computer networks (1 of 2)



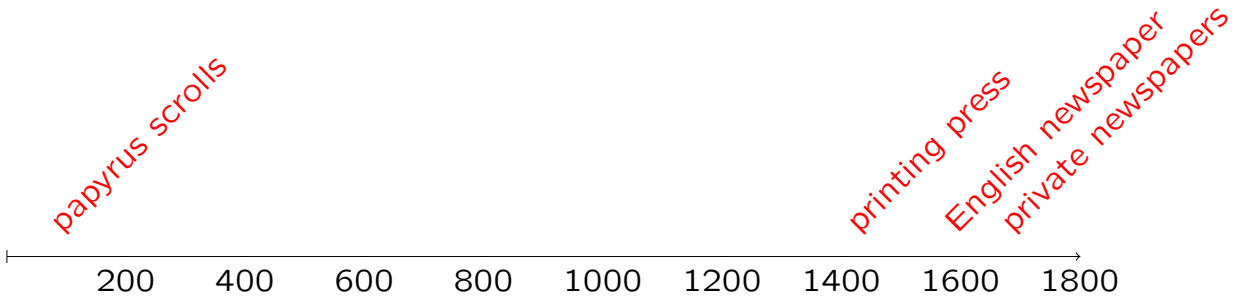
- In 1957, the U.S. Department of Defense created the Advanced Research Projects Agency (ARPA).
- In 1960, modems were developed, to transmit digital data over a telephone.
- In 1969, ARPA teams formed the ARPANET by connecting University of California Los Angeles and Santa Barbara, Stanford Research Institute, and University of Utah.
- In 1972, an email program for ARPANET was written.

Computer networks (2 of 2)



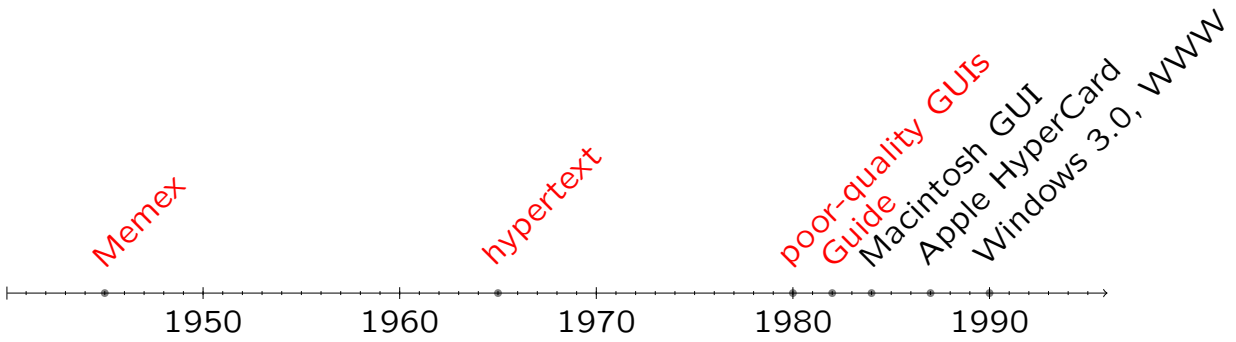
- In 1983, ARPANET hosts converted to a protocol called TCP/IP, spawning the Internet.
- Regional networks were connected to NSFNET, a noncommercial backbone sponsored by the National Science Foundation. Private companies developed commercial backbones.
- Initially, residential Internet access was through a modem and telephone line. Since phones were designed to transmit voice, bandwidth was low. Higher-speed access is now available over telephone, cable-television, and other systems (i.e., broadband).

Early storage



- Before the year 200, data was stored on papyrus scrolls. The *codex* was an early improvement. It was a sequence of sheepskin or calfskin "pages," sewn together on one side.
- In 1436, Gutenberg's metal-type printing press was developed.
- In the 1600s, the first English newspaper appeared.
- In 1695, non-government newspapers began.

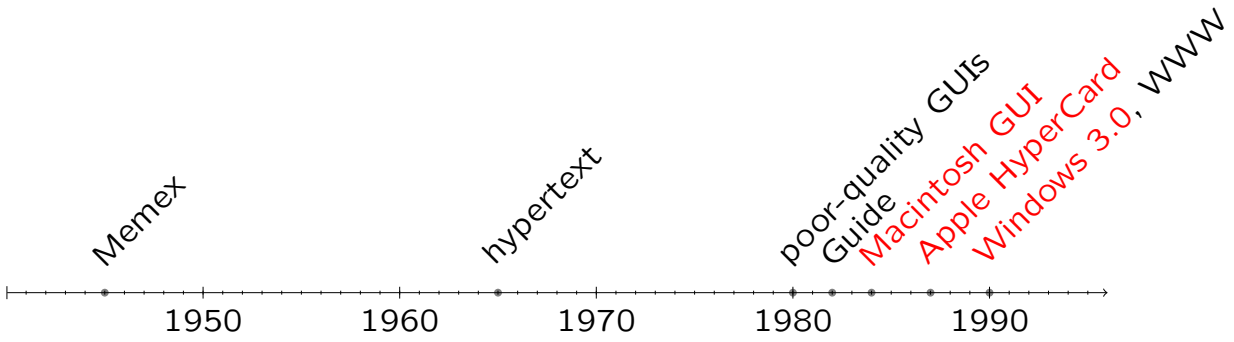
Hypertext, GUIs, and searching (1 of 3)



- In 1945, a data-indexing system named Memex was described.
- In 1965, these ideas were refined and called *hypertext*, a linked system of nodes that could be visited in a nonlinear way.
- During the 1980s, poor-quality GUIs were available for IBM PC clones.
- One-computer hypertext systems came first. In 1982, a system named Guide was developed, for Apple and IBM PCs.

  pub/ch1/guide.jpg

Hypertext, GUIs, and searching (2 of 3)



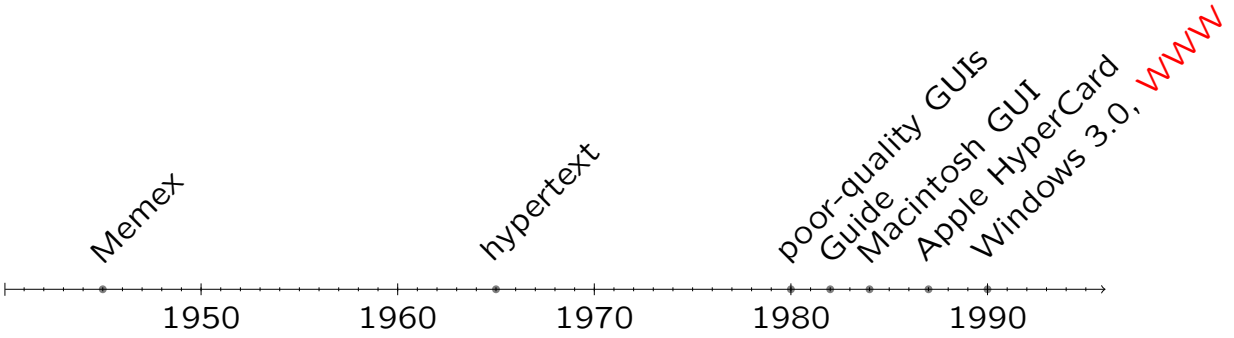
- In 1984, Apple released its Macintosh, with a GUI.

  pub/ch1/mac.jpg
- In 1987, Apple released HyperCard.

  pub/ch1/hypercard_welcome.jpg
- In 1990, Microsoft released Windows 3.0, and consumers bought 10 million copies.

  pub/ch1/1ibm5170.jpg

Hypertext, GUIs, and searching (3 of 3)



- In 1990, Tim Berners-Lee finished a program that could traverse hypertext data that spanned multiple computers, across a TCP/IP network. Both his parents were programmers for the Ferranti Mark I computer in the 1950s. He called his *browser* WorldWideWeb (WWW).
- Web *search engines* are systems that create an index of website data, by following links. They allow a user to search the index for words or phrases.

Information technology issues (1 of 2)

- The term *information technology* (IT) refers to a broad collection of devices and methods for processing data. IT has been rapidly getting better and cheaper.
- However, these changes cause problems and raise questions. Here are few of them:
  - Email is an effective way to communicate, but about 90% of it is *spam*: unsolicited, bulk, commercial email.
  - The WWW is international. How do state and national laws apply?
  - Digital data has strange economies. The first instance can be outrageously difficult and expensive to produce, but copies can be made for nearly free. How can ownership rights be preserved?

Information technology issues (2 of 2)

- IT activity is easy to log. How can privacy rights be preserved?
- Many people and groups contribute to an IT artifact, perhaps without knowing what the artifact is. For example, many medical devices contain hardware and software produced by different companies. How can this distributed liability be assigned? Who is responsible for a failure that kills many people?
- Is telecommuting good?
- Is offshore outsourcing good?
- Should a government be able to monitor and censor Internet data?

Chapter 2: Introduction to Ethics (1 of 2)

- People live in families, and families live in communities. By living in a group, a person can specialize, be more productive, and enjoy a better life.
- Every group requires certain behaviors and prohibits certain behaviors. Thus, living in a group restricts a person's freedom.
- Evidently, the benefits of living in a group are greater than the costs.
- A group's requirements tend to promote the welfare of the group as a whole, rather than particular members. Each requirement is expressed as a rule (e.g., a member must not kill another person).

Introduction to Ethics (2 of 2)

- Sometimes, a behavior is difficult to categorize as good or bad. Perhaps, the rules are inconsistent or incomplete. Perhaps, there are unforseen circumstances. In these cases, an abstract behavioral guideline, an *ethical theory*, can be used to analyze a behavior.
- Of course, there is more than one ethical theory. We will study several popular theories, and learn to use them to analyze questionable behaviors.

Defining terms

- A *society* is a group of people organized under a set of such rules.
- Each rule is called a *moral*.
- The set of rules is called *morality*.
- Behavior according to the rules is *moral*, otherwise it is *immoral*. A person can belong to multiple societies, which can cause moral conflict.
- *Ethics* is the philosophical, rational, and objective study of morality.

Four scenarios (intro)

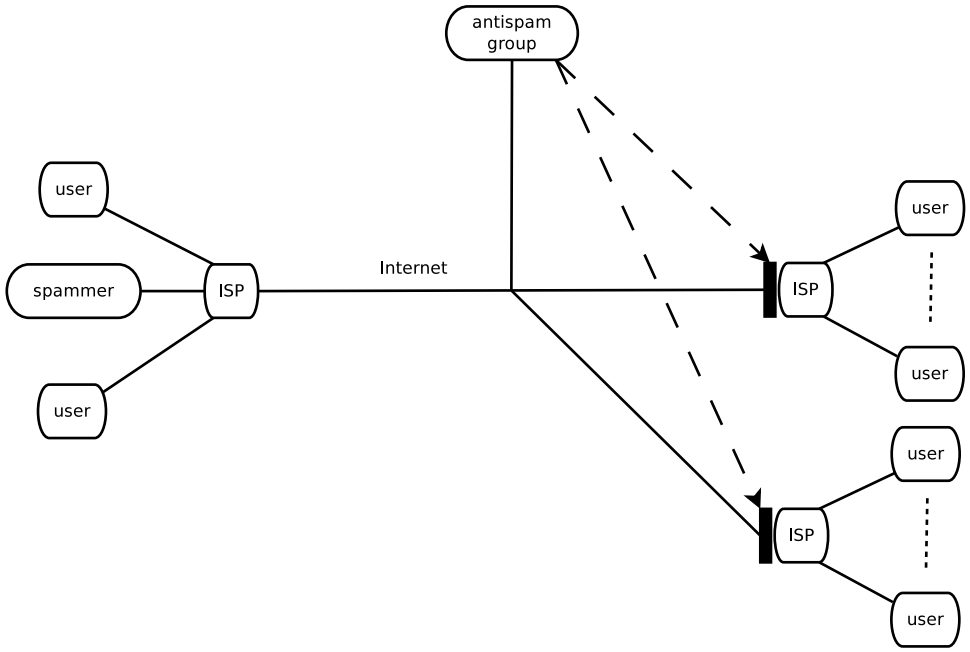
- Our textbook presents four scenarios with ethical questions. Read them for details.
- While thinking about a scenario, consider the mental process you use to answer questions about it. How would you explain your answer to someone who disagrees? Ethics provides this framework.
- Ethics is focused on voluntary moral choices. An involuntary choice is not a moral choice. For example, hitting a pedestrian with your car because you reflexively swerved to avoid another pedestrian is not a moral choice. However, hitting a pedestrian while texting is a moral choice. Likewise, picking your favorite color is a not a moral choice.

Scenario: library

- A high school student wants to study to win a scholarship. Her library's resources are poor and overused, and she works after school. She uses resources in a private college library, telling the librarian that she is a student there. She wins the scholarship.

Scenario: spam

- An antispam group blacklists an Internet service provider (ISP), which refuses to cooperate.
- Many other ISPs use the blacklist.
- Spam is significantly reduced, but the ISP's other users cannot send email.



Scenario: speeding

- State police install cameras that automatically ticket speeding drivers.
- Speeding is reduced by 90%.
- Later, the FBI uses the data to arrest suspected terrorists.

Scenario: software

- Your company is developing smartphone software.
- It is almost done. The known bugs are minor.
- However, more testing is needed, which could find catastrophic bugs.
- A competitor is about to release a similar system. The first company to release will probably put the second company out of business.

Overview of ethical theories

- Ethics is at least 2,400 years old, starting with Plato writing about Socrates.
- Since then, many ethical theories have been developed.
- Such a theory is useful if it can help us analyze moral problems and defend our conclusions.
- It must allow us to give a sequence of logical reasons that lead to our conclusion.
- We will consider nine ethical theories. According to our textbook:

  > The workable theories will be those that make it possible for a person to present a persuasive, logical argument to a diverse audience of skeptical, yet open-minded people.

- We will discard the other theories.

Subjective relativism

- *Relativism* is the theory that there are no universal morals. We will see two kinds of relativism: subjective and cultural.
- *Subjective relativism* is the theory that right and wrong is a personal decision.
- For:
  - Two people can have opposite morals.
  - Ethical debate is pointless: both sides are right.
- Against:
  - Immoral behavior can be easily rationalized: A person can claim moral behavior regardless of his/her beliefs.
  - The behavior of different people cannot be compared.
  - It is not the same as tolerance.
  - It is not based on reason.
- For these reasons, we reject subjective relativism as a workable ethical theory.

Cultural relativism (1 of 2)

- *Cultural relativism* is the theory that right and wrong is a decision made by a group of people, community, or society. We all know that different cultures have different morals.
- For:
  - Differences in culture require different morals
  - A member of one group cannot fully understand another group.
  - The actual behavior of a group is a more accurate depiction of its morals than a hypothetical description.

Cultural relativism (2 of 2)

- Against:
  - One group's moral behavior could be considered immoral by every other group.
  - It does not explain how a member learns the group's morals.
  - It does not explain how a behavior's morality can change over time.
  - It does not explain how to resolve intergroup conflicts.
  - The fact that many opposing behaviors are moral, in different groups, does not imply that any such behavior is moral.
  - Some morals are universal.
  - It is only indirectly based on reason: some morals are just traditions.
- For these reasons, we reject cultural relativism as a workable ethical theory.

Divine command theory (1 of 2)

- Many societies are organized around religions. Many religions have sacred texts, sometimes containing the will of the religion's idea of God (e.g., a Christian bible).
- The *divine command theory* says that a religion's texts specify morality. For example, if God says do not kill a person, killing a person is bad.
- For:
  - A religious person owes obedience to the religion's God.
  - A religion's God is knowledgeable and good.
  - A religion's God is the ultimate authority.

Divine command theory (2 of 2)

- Against:
  - There are many, contradictory, religious texts, even for a single religion.
  - A group is unlikely to embrace a single religion.
  - A religious text may be incomplete, and difficult to extrapolate to the problem being analyzed (e.g., the Jewish Torah and Talmud).
  - Does a religious text describe good, or define good? If it describes good, what defines it? If it defines good, what is the reasoning, or is good arbitrary?
  - It is based on obedience, not reason.
- For these reasons, we reject divine command theory as a workable ethical theory.

Ethical egoism (1 of 3)

- *Ethical egoism* is the philosophy that each person should focus exclusively on his or her self-interest. The morally right action for a person is that which provides that person with the greatest long-term benefit.
- This theory does not preclude helping others, but only if that is a side effect of helping yourself. For example, you might help a friend fix his car, but only if he has been driving you to work.

Ethical egoism (2 of 3)

- For:
  - It is practical. In many ways, a person is responsible for his or her own survival.
  - A community can benefit when individuals benefit. For example, a successful business person may claim to create jobs for the community.
  - Other moral principles are rooted in self-interest. For example, community cooperation also benefits individuals.

Ethical egoism (3 of 3)

- Against:
  - An easy theory may not be a good theory.
  - Many people do not naturally act in their own long-term benefit.
    Short-term benefits are too tempting.
  - Disproportionate individual benefits can harm a community. Slavery is an example.
  - Even a tiny personal benefit outweighs any community benefit.
  - It is bigotry. An individual has higher moral status than any other individual, which cannot be true for everyone.
- For these reasons, we reject ethical egoism as a workable ethical theory.

Kantianism (1 of 6)

- This theory is named after Immanuel Kant (1724-1804). He believed that behavior should be guided by universal morals. In order to apply to all rational people, they must be based on reason. His theory can explain why behavior is right or wrong.
- His theory says that the only universal good is a good will or intent. Consequences are of of no importance.
- The focus should be on duty: what a person ought to do, according to an appropriate moral.

Kantianism (2 of 6)

- What makes a moral appropriate? Kant proposed the *Categorical Imperative*, of which our textbook has two formulations:
  - Act only according to morals that you can at the same time will to be universal.
  - Act so that you always treat both yourself and other people as ends in themselves, and never only as a means to an end.
- As an example, we can use this theory to evaluate the behavior:

  A person makes a false promise (i.e., lies), because that is the only way to escape a difficult situation.

Kantianism (3 of 6)

- To universalize it, consider what would happen if everyone made false promises: nobody would believe promises. Then, our liar would not be able to escape the situation. Therefore, the behavior is immoral.
- Note that the theory is not labeling the behavior immoral because it leads to bad consequences. It is immoral because it leads to a logical contradiction.

Kantianism (4 of 6)

- As another example, consider a hiring manager at a factory.
- The manager knows the factory will close in a year. Should the manager withold this information from out-of-state applicants, to increase the chance they will relocate?
- Witholding the information treats applicants as a means to staff the factory for a year, rather than as people. Thus, the behavior is immoral.

Kantianism (5 of 6)

- As another example, consider a single-mom student, enrolled in a class requiring four term papers.
- She receives an A on her first three papers, but buys the fourth paper from a website. Is this immoral?
- If everyone bought their papers, professors would not assign them, and her attempt could not happen.
- Furthermore, she is treating her professor as a grade-generating machine, rather than as a person.
- Thus, her behavior is immoral.

Kantianism (6 of 6)

- For:
  - It is rational.
  - It produces universal morals.
  - People are treated equally.
- Against:
  - Sometimes, a behavior is addressed by multiple morals. Which should be universalized? For example, is stealing to feed your family immoral?
  - Conflicts between morals cannot be resolved.
  - No exceptions are allowed. For example, consider "white" lies.
- We accept Kantianism as a workable ethical theory.

Act utilitarianism (1 of 5)

- In contrast to Kant's theory, Jeremy Bentham (1748-1832) and John Stuart Mill (1806-1873) developed the theory of *utilitarianism*.
- This theory is based on the *Principle of Utility*:

  > A behavior is right (wrong) depending on whether it increases (decreases) the total happiness of the affected parties.

- To analyze a behavior, the change in happiness is "computed" for each affected person. If the net change is positive, the behavior is moral, otherwise it is immoral.

Act utilitarianism (2 of 5)

- Note that the theory does not consider the will or intent of a behavior. All that matters is the result. It is a *consequentialist* theory.
- When performing the utilitarian "calculus," what happiness is measured?
  - only adult white males?
  - all humans?
  - all animals?
  - plants, too?
  - aspects of the Earth's environment?

  What is the unit of measure? For example, how unhappy is a polluted river?

Act utilitarianism (3 of 5)

- Suppose a state's government is considering a project to rebuild a curvy stretch of highway. Would this be a moral behavior?
  - It condemns some homes (sad).
  - It is expensive (sad).
  - It damages the environment (sad).
  - It provides jobs (happy).
  - The shorter road reduces travel expenses (happy).
  - The straighter road reduces accidents (happy).
- The hard part is to quantify costs and benefits, perhaps in dollars. Then, the comparison is simple.

Act utilitarianism (4 of 5)

- Several attributes can be considered when trying to quantify costs and benefits of an experience:
  - *intensity*: how strong it is
  - *duration*: how long it lasts
  - *certainty*: the probability it happens
  - *propinquity*: proximity
  - *fecundity*: whether it repeats itself
  - *purity*: whether it is diluted by its opposite
  - *extent*: how widespread it is
- For:
  - It focuses on happiness.
  - It is practical, objective, and rational.
  - It is comprehensive.

Act utilitarianism (5 of 5)

- Against:
  - The scope of the utilitarian calculus is difficult to select.
  - Performing the calculus can be expensive, in time and effort.
  - It ignores our sense of duty.
  - The predicted consequences may not occur.
- We accept act utilitarianism as a workable ethical theory.

Rule utilitarianism (1 of 4)

- While act utilitarianism performs a happiness calculation on a particular instance of a behavior, *rule utilitarianism* universalizes the calculation to consider the costs and benefits resulting from everyone behaving that way.
- Rule utilitarianism considers the consequences of a rule, while Kantianism considers the motivation behind a rule.
- Here's an example: In 2003, the Blaster virus spread through the Internet, causing infected hosts to reboot every few minutes. Soon after, the Nachi virus spread through the Internet, exploiting the same OS vulnerability. However, when Nachi infected a host, it removed any Blaster infection and fixed the vulnerability.

Rule utilitarianism (2 of 4)

- Clearly, releasing Blaster was immoral. What about Nachi?
  - It removed Blaster and fixed vulnerabilities (happy).
  - Many Nachi-like viruses would increase network traffic (sad).
  - A Nachi-like virus could contain bugs that damage infected hosts (sad). In fact, Nachi disabled some ATMs. The more such viruses there are, the more likely such bugs exist.
  - Until a virus is identified, a system administrator must assume it is a bad one (sad).

  Thus, rule utilitarianism calls the release of Nachi immoral, even though act utilitarianism might call it moral.

Rule utilitarianism (3 of 4)

- For:
  - The calculus for rule utilitarianism is simpler than for act utilitarianism.
  - Once a rule is deemed moral, individual behaviors need not be analyzed.
  - Exceptional act calculations are absorbed by many applications of the rule. For example, the cost and benefit of a particular act might be nearly the same.
  - Likewise, exceptional consequences are absorbed by many applications of the rule. For example, sending flowers to someone in the hospital is moral, even though a few people might be allergic to them.
  - It appeals to many people, like the phrase: "It's all right to do anything as long as no one gets hurt."

Rule utilitarianism (4 of 4)

- Against:
  - The unit of measure is difficult to select.
  - While the benefits may outweigh the costs, they may not be distributed equitably among the participants.
- We accept rule utilitarianism as a workable ethical theory.

Social contract theory (1 of 9)

- This ethical theory was developed by Thomas Hobbes (1603-1679) and, later, by Jean-Jacques Rousseau (1712-1778).
- The theory says that people living in a civilized society have agreed to:
  - a set of rules governing relations among members
  - allow a government to enforce these rules

  Without rules, and enforcement, people would live in *a state of nature*: They would not create anything of value, because they could not keep what they created.

Social contract theory (2 of 9)

- This is our textbook's statement of the theory:

  > Morality consists in the set of rules, governing how people are to treat one another, that rational people will agree to accept, for their mutual benefit, on the condition that others follow those rules as well.

- According to the theory, a rule need not be universalizable to be moral, as with Kantianism. Instead, the rule must be collectively acceptable to the society, because of its societal benefits.
- Social contract theory introduces *rights* and *duties*, which are related as duals. If one person has a right, others have a duty ensure it.

Social contract theory (3 of 9)

- A *negative right* is one others can ensure by not interfering (e.g., a right to privacy).
- A *positive right* is one that requires action from others (e.g., a right to a free education).
- An *absolute right* is ensured without exception (e.g., a right to life).
- A *limited right* may be restricted, due to circumstances (e.g., a right to a free education, limited to grades K-12).
- Positive rights are typically limited rights.

Social contract theory (4 of 9)

- Social contract theory recognizes that wealth concentration can be harmful. Rousseau wrote:

  > The social state is advantageous to men only when all possess something and none has too much.

- John Rawls (1921-2002) extended social contract theory to address unequal distribution of wealth and power.

Social contract theory (5 of 9)

- He defined two *Principles of Justice*:
  - A person may claim basic rights, only if they are consistent with everyone claiming them.
  - Any inequities must satisfy two conditions:
    * they are associated with positions in society that everyone has a chance to assume
    * they are to be most greatly beneficial to the least advantaged

  This last clause is called the *Difference Principle*.

Social contract theory (6 of 9)

- An example of the Difference Principle is the graduated income tax, where rich people pay a higher percentage of their income.
- An example that violates the principle is a military draft that excludes rich people.
- Of the first 240,000 drafted into the military between 1966 and 1968, 40% read below sixth-grade level, 41% were black, 75% came from low-income families, 80% had dropped out of high school.
- Secretary of Defense McNamara said: "The poor of America have not had the opportunity to earn their fair share of this nation's abundance, but they can be given an opportunity to serve in their nation's defense."

Social contract theory (7 of 9)

- Suppose a retailer keeps a record of customer purchases, and sells it to mail-order companies. The mail-order companies send catalogs to the customers.
- Some people like the catalogs, others do not. Is the retailer's behavior moral?
- The retailer has a right to the transaction data. The customers have a right to privacy. Whose rights are greater, to society as a whole?
- Probably, the right to privacy would be more important.

Social contract theory (8 of 9)

- For:
  - It is based on rights, which people find attractive.
  - It explains why rational people act selfishly, without an agreement to act otherwise.
  - It explains the relationship between people and government.

Social contract theory (9 of 9)

- Against:
  - No one signed the social contract. If you do not agree, you must leave society.
  - Identifying rights that apply to a behavior can be difficult. Different people may choose different rights.
  - Rights may conflict. Consider abortion: The mother has a right to privacy and some people claim the fetus has a right to life.
  - Do people who act immorally retain their rights? For example, do prison inmates have a right to privacy?
- We accept social contract theory as a workable ethical theory.

Virtue ethics (1 of 6)

- Some philosophers believe that previous theories ignore:
  - moral education
  - moral wisdom
  - family and social relationships
  - the role of emotions
- *Virtue ethics* accounts for these factors.
- Virtue ethics can be traced back to ancient Greece. Here, *virtue* means excellence and reaching one's highest potential. The path to happiness and flourishing as a human lies in living a life of virtue.

Virtue ethics (2 of 6)

- A *moral virtue* is a deep-seated character trait, attained by repetition of a virtuous action.
- Aristotle identifies about two dozen moral virtues (e.g., prudence, justice, fortitude, temperance, generosity, patience, honesty, friendliness, modesty, and wittiness).
- Consider honesty. A person becomes honest by living a life free of dishonest actions. At first, honesty is learned. Eventually, honesty is automatic and second nature. Dishonesty causes discomfort.
- With virtue ethics, morally good people consistently do what is right. They don't decide to *act* a particular way. They are disposed to *feel* a particular way. Good behavior is connected to emotions.

Virtue ethics (3 of 6)

- A *vice* is the opposite of a virtue.
- Consider the virtue of bravery. Too much is a vice: recklessness. Too little is a vice: cowardice.
- Consider the virtue of friendliness. Too little might lead to petty quarrels. Too much might lead to a lack of needed criticism.

Virtue ethics (4 of 6)

- Suppose a college course requires students to work on a team project. One team include friends Josh and Matt. Josh is indebted to Matt for rides to school. During the semester, Matt's dad dies, and Matt disconnects from Josh and the project. Josh and the rest of the team cover for Matt.
- At the end of the semester, students must "grade" their teammates. Josh could:
  - report that Matt's work was fine
  - report that Matt did not do the work
  - give the instructor a full account of what happened, including his (Josh's) failure to help earlier

Virtue ethics (5 of 6)

- For:
  - Virtues often make more sense than obligations, rights, or consequences. For example, stealing for selfish reasons is wrong because it is contrary to the virtue of honesty.
  - Relationships can be relevant to decision making. For example, parents treat their children in different ways than other children.
  - It recognizes that our decision-making skills develop over time.
  - There are no irresolvable moral dilemmas. There may be hard choices, but enough moral wisdom allows the right choice to be made.
  - It recognizes that emotions are important. People are not calculating machines.

Virtue ethics (6 of 6)

- Against:
  - People disagree on the virtues: the character traits we need to flourish as humans.
  - It cannot guide government policy. It guides an individual's behavior.
  - It does not hold (all) people responsible for bad actions. Since virtues and vices are acquired over time, from parents and teachers, how can we blame a person who has vices?
- Virtue ethics isn't perfect, but it provides a framework for moral analysis, so we conclude that it is a workable ethical theory.

Comparing workable ethical theories (1 of 2)

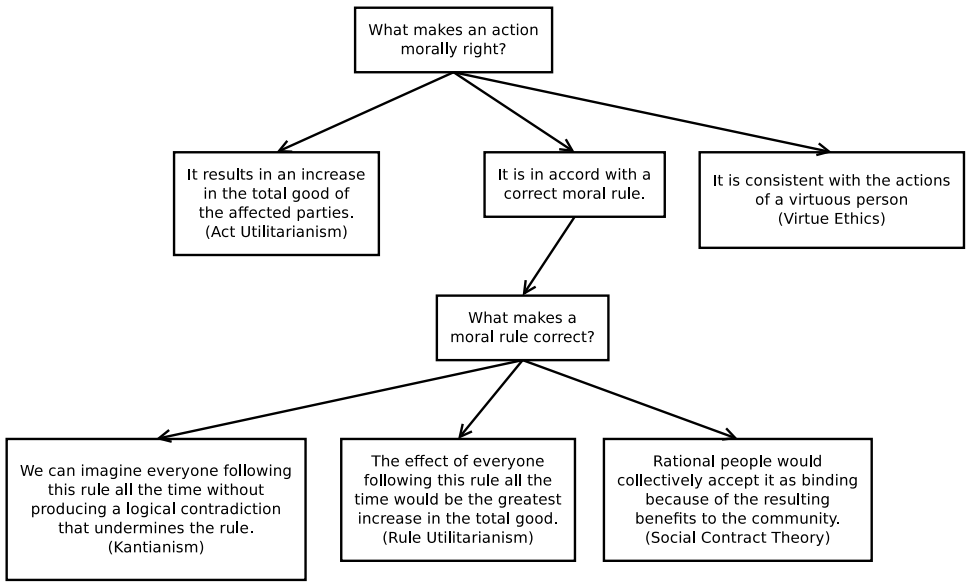
- Our five workable ethical theories allow people to discover objective moral principles, with logical reasoning, based on facts and commonly held values. They are examples of *objectivism*.
- We can summarize the differences between the five theories:
  - What is the motivation for an action? Is it based on intent, consequences, rights, or character?
  - What criteria determines whether a behavior is moral or immoral? Is morality universal or based on a computation?
  - Is the focus on an individual or the group?

Comparing workable ethical theories (2 of 2)

- Table 2.1, in older editions, summarizes this data:

Theory	*Motivation*	*Criteria*	*Focus*
Kantianism	intent/duty	rules	individual
Act Utilitarianism	consequence	actions	group
Rule Utilitarianism	consequence/duty	rules	group
Social Contract	rights	rules	individual
Virtue Ethics	character	virtues	individual

- Here's a flowchart comparison:



Morality of breaking the law (1 of 2)

- The intersection of morality and law is typically large, but some law-abiding behavior might be immoral (e.g., the death penalty), and some possibly moral behavior is illegal (e.g., abortion-clinic confrontations).
- For example, consider giving a friend a copy of a copyrighted music CD. This act is illegal.
- According to social contract theory, the rights of the copyright holder are violated, so the act is immoral.
- According to Kantianism, if everyone illegally copied CDs, recording companies would not produce them, so there would not be a CD to copy. This is a contradiction, so the act is immoral.

Morality of breaking the law (2 of 2)

- According to rule utilitarianism, the consequences of everyone making illegal copies would hurt the recording companies more than it would help the copy recipients. Again, the act is immoral.
- According to act utilitarianism, we need only calculate costs and benefits of a particular violation of the law. For example, if the recipient would never have bought the CD, the cost to the record companies is zero. Now, the act is moral. Beyond that, circulating a few illegal copies might provide positive publicity that benefits the record companies. Even more, the act is moral.
- According to virtue ethics, the act is dishonest, and thus immoral.

Chapter 3: Networking

- An isolated computer can be useful, but sharing resources with other computers makes it far more useful. Some example resources are printers, storage devices, processors, and databases.
- Generally, increasing the number of networked computers increases each computer's usefulness. For example, email is only effective if the people you want to communicate with have networked computers.
- Conversely, network utility decreases in at least two cases:
  - when its data-carrying capacity is exceeded
  - when its users misbehave
- This chapter focuses on ethical aspects of the Internet: email and its abuse (e.g., spam), censorship, freedom of expression, fraud, and addiction.

How email works (1 of 3)

- An *email message* is a file that is transferred from one computer to another, across a network, according to an email address.
- The message and address is specified by Request For Comments 822 (RFC 822).
- RFCs are open documents that record the discussion and development of new protocols and techniques for use on the Internet.
- The process is now run by the all-volunteer Internet Engineering Task Force (IETF).
- If you want to learn Internet etiquette (netiquette), read RFC 1855.

How email works (2 of 3)

- In general, an *email address* specifies a computer on the Internet and a user on that computer.
- A message can be sent to a user on the sender's computer, by not specifying a destination computer.
- There is also an address syntax for specifying a route by which the destination computer can be reached.

How email works (3 of 3)

- Typically, a computer is specified by its symbolic *domain name* (e.g., `onyx.boisestate.edu`).
- A domain name is "resolved" into a numeric *Internet-Protocol* (IP) address (e.g., `132.178.227.11`), by the *Domain Name System* (DNS). DNS is specified by a set of RFCs.
- An email message is transferred from computer to computer as a sequence of *packets*: fairly independent chunks of data. They may traverse multiple computers along different routes. They may even arrive at their destination out of order.

The spam epidemic (1 of 3)

- Over 200 billion email messages are sent each day.
- Many of these messages are unsolicited, bulk, commercial email: spam.
- In 2000, 8% of email was spam. In 2009, 90% was spam.
- Recall that the Internet began as a noncommercial academic network. In 1994, a couple of lawyers from Phoenix spammed 9,000 Usenet newsgroups with an email advertisement.
- Today, estimates claim that spam costs billions of dollars a year in wasted productivity.
- The economics of spam are surprising. A spammer can make make a profit even if only one in 100,000 recipients buys the product.

The spam epidemic (2 of 3)

- Spammers can guess email addresses, or they can buy them from other, disreputable, companies.
- Companies and ISPs can try to block spam, with filters. The filtering computer still has to process spam, but ordinary users are spared. Of course, spam can fool a filter, and a filter can block non-spam messages.
- A spammer can easily hide or falsify a return address. This is called *spoofing*.
- A return address can also be changed to some other legitimate address, thereby harassing the owner of the spoofed address.

The spam epidemic (3 of 3)

- An insecure computer can be compromised and turned into a spam-sending computer, a *bot*, leaving its owner oblivious to the problem (for a while).
- Typically, this is done to a large number of computers, forming a *botnet*.

Ethical evaluation of spamming (1 of 5)

- Most people hate spam, but does that make spamming immoral behavior? We can analyze a spammer's behavior according to the ethical theories we discussed in Chapter 2.
- Consider Kantianism:
  - The spammer is trying to reach the small fraction of recipients who want to buy the product. As a means to that end, the spammer causes all other recipients the expense and inconvenience of processing the spam. The spammer is using almost every recipient as a sales aid.
  - If everyone sent spam, the Internet would fail and no one could send spam.

  Thus, spamming is immoral.

Ethical evaluation of spamming (2 of 5)

- Consider Act Utilitarianism. Our textbook proposes monetary costs and benefits, but let's be qualitative:
  - The spammer profits (happy).
  - Some customers like the product (happy).
  - Some customers do not like the product (sad).
  - Most likely, all non-customer recipients incur the expense and inconvenience of processing the spam (sad).

  Since the cost of the last item greatly exceeds all benefits, spamming is immoral.

Ethical evaluation of spamming (3 of 5)

- Consider Rule Utilitarianism. This is similar to the analysis of Act Utilitarianism. However, here are two differences:
  - Suppose an occasional spam campaign promotes a good product at a good price. Many recipients would want the product, but the spammer would be able to make only a few of them happy.
  - If spamming becomes more common, people will stop using email, thereby making email less effective for everyone.

  Again, spamming is immoral.

Ethical evaluation of spamming (4 of 5)

- Consider Social Contract Theory. In many societies, a person has a right to free speech. However, other people have a right not to listen. When a spammer forces a person to process an unwanted email message, the recipient is being forced to listen to the message, at least long enough to identify it as spam. According to this theory, rules allowing spamming must be collectively acceptable to the society, because of its societal benefits. Spamming does not fit this criteria, and is immoral.

Ethical evaluation of spamming (5 of 5)

- Consider Virtue Ethics. Does spamming contribute to personal excellence and reaching one's highest potential? No, hardly.
- Can spam be made moral? These changes to spam would change our theoretical analyses:
  - Use accurate return addresses.
  - Use accurate subject lines.
  - Send only to people who request it.

Real-time blackhole list (RBL) (1 of 4)

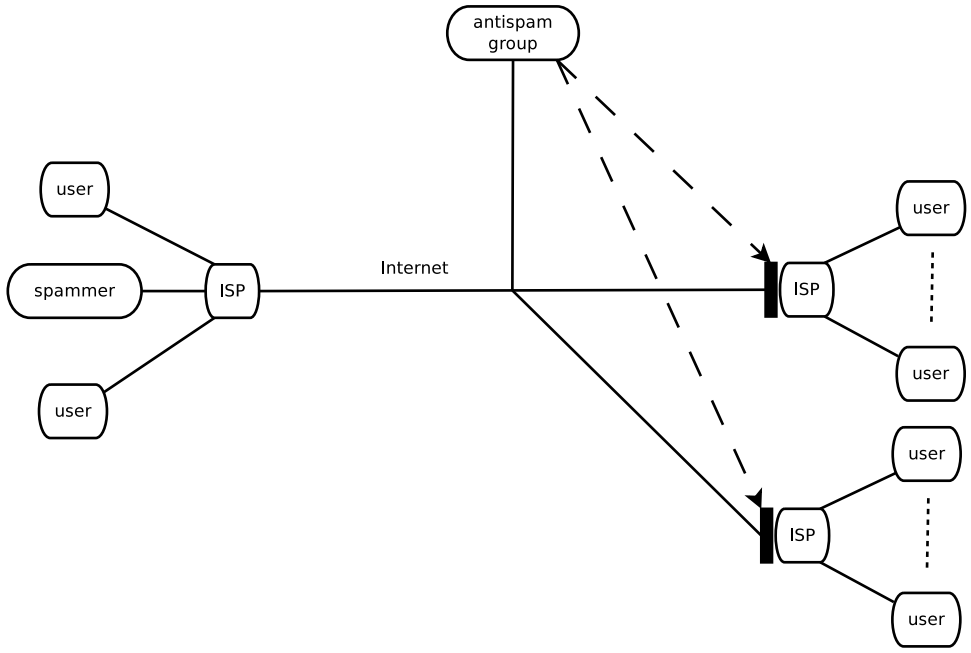
- A spam filter analyzes the content of a message to determine whether it is spam.
- Another approach is to maintain a set of IP addresses suspected of sending spam.
- When a message is received from one of these addresses, it is not forwarded (i.e., it is consumed by a "black hole").
- The set of addresses changes as suspect spammers are added or removed.

Real-time blackhole list (RBL) (2 of 4)

- An IP address can be added to an RBL for several reasons:
  - Spam has been sent from it.
  - Spammers use it in other ways.
  - Its mail server is unsecured or misconfigured (e.g., configured as an "open relay" that might forward spam from another mail server).
  - It is dynamically assigned.
- Note that an address that has never sent spam can be added to an RBL. There is an online mechanism to correct such mistakes, after the cause has been fixed.

Real-time blackhole list (RBL) (3 of 4)

- There are several relevant parties:



  - spam sender
  - other senders
  - senders' ISP
  - RBL maintainer
  - receivers' ISP
  - receiver
  - other receivers

Real-time blackhole list (RBL) (4 of 4)

- The receivers' ISP can subscribe to the RBL and configure its mail server to check incoming mail against the list.
- A match is blocked as spam.
- The problem is that all of the senders' messages are blocked, spam or not, because the RBL contains the IP address of the spam sender's ISP.

Ethical evaluation of RBLs (1 of 3)

- Is the RBL maintainer's behavior moral?
- Note that we are not considering the behavior of the spammer or either ISP.
- Consider Social Contract Theory. The RBL maintainer has a right to free speech. The maintainer is publishing information about particular IP addresses. The criteria is clear, the data is very accurate, and there is a mechanism for correcting errors. The maintainer does not force an ISP to use the RBL in any particular way. So, the behavior is moral.

Ethical evaluation of RBLs (2 of 3)

- Consider Act/Rule Utilitarianism. There are costs and benefits:
  - Receivers receive less spam (happy).
  - Receivers see better performance (happy).
  - Spammer is blocked (sad).
  - Non-spamming senders are blocked (sad).
  - Receivers do not receive blocked nonspam messages (sad).
  - Misconfigured mail servers are fixed (happy).
  - ISPs regulate their customers (happy).

  The degree to which legitimate users are negatively affected by blacklisting determines the morality of maintaining the RBL. A blacklisted legitimate sender can complain to their ISP or switch ISPs. However, there are usually few choices.

Ethical evaluation of RBLs (3 of 3)

- Consider Kantianism:
  - What if everyone maintained an RBL? Collectively, there would be more errors than in a single, expertly maintained, RBL. Also, errors would be more difficult to remove from all of them. This could cause a significant decline in email use, rendering RBLs unneeded.
  - Is the RBL maintainer treating anyone as a means to an end? Blacklisted legitimate senders are being used to reduce spam. Granted, they might complain to their ISP or switch ISPs.
  - So, creating an RBL is immoral.
- Consider Virtue Ethics. Are the RBL maintainers seeking, for example, justice and honesty? Yes.

Proposed solutions to the spam epidemic (1 of 2)

- There are several proposals:
  - Allow messages to be sent only to people who have explicitly agreed to receive them.
  - Require a subject line that identifies the content. This simplifies automatic and manual filtering.
  - Charge the sender a small amount of money for each message. This fixes the strange economy of spam.
  - Ban spam. This is like the 1991 law banning unsolicited faxes.

Proposed solutions to the spam epidemic (2 of 2)

- There are newer techniques:
  - Require a sender to "register" with the receiver.
  - Use a trademarked message header.
  - Sender Policy Framework (SPF): The receiver performs a DNS lookup on the sender's (possibly spoofed) domain name to determine if the sender's IP address is allowed to send email from that domain.
  - DomainKeys Identified Mail (DKIM): The receiver performs a DNS lookup on the sender's (possibly spoofed) domain name to obtain a public key, which is then used to check a private-key signed header in the email.

CAN SPAM Act of 2003
(1 of 3)

- This U.S. law is an acronym for Controlling the Assault of Non-Solicited Pornography And Marketing.
- It partitions *legal* commercial email into three sets:
  - Transactional messages continue an ongoing relationship between parties. Headers and content must be accurate. The sending address must be identified.
  - Commercial messages are those that the recipient has agreed to receive. In addition to the previous requirements, the message must describe an Internet-based mechanism for removing the recipient from the mailing list. It must also contain the postal address of the sender.

CAN SPAM Act of 2003
(2 of 3)

  - Unsolicited commercial email messages. In addition to the previous requirements, the message must describe the content as commercial or sexually explicit.
- The law includes fines of $250 per email, with a limit of $2 million, or $6 million for repeat offenders. It also sets prison terms for people who setup spambots or spoof email headers.

CAN SPAM Act of 2003
(3 of 3)

- Critics of the law say it legalizes spam. If 1% of U.S. small businesses sent you one message per year, you would receive over 600 spams per day.
- It is weaker than many state laws. It does not apply to foreign spammers.
- If you remove yourself from a mailing list, the owner can sell your (validated) address to another list owner.
- A 2004 study found 14% of spam following the law.
- A 2006 study found 6% of spam following the law.

Attributes of the World Wide Web

- The WWW has become the most important data storage and retrieval system.
- It is decentralized. Anyone with a computer with an Internet-accessible IP address can create WWW pages.
- Each WWW object has a unique address, called a Uniform Resource Locator (URL).
- The WWW is based on the Internet, making it platform neutral. Different kinds of CPU and OS interoperate.

How we use the web
(1 of 2)

- We buy. This is remarkably convenient.
- We socialize. We can exchange email and instant messages. Social-networking sites provide more complex relationships.
- We contribute. You can add text, photos, and videos for other people to view.
- We blog. A "web log" is an online journal, documenting a person's experiences.
- We sell. You can simply describe your business, or perform complex transactions.
- We learn. Search engines can quickly answer many questions. Also, you can enroll in online classes.
- We play. There are many online games. Some let you interact with other people. Some people make money playing games.

How we use the web
(2 of 2)

- We pay taxes. Many people file electronically, receiving their refund sooner.
- We gamble. This generates $6 billion per year. Since most states prohibit gambling, these sites are outside of the U.S.

Too much governmental control or too little?

- A government can limit a citizen's access to the Internet in several ways:
  - Myanmar (Burma), Cuba, and North Korea block international access.
  - Saudi Arabia has a filtering center, which blocks pornography, gambling, and other content the government considers offensive (e.g., music and movies).
  - China requires all ISPs to block content the government considers offensive (e.g., CNN).
  - Germany blocks access to neo-Nazi sites.
  - The U.S. criminalizes access of certain content (e.g., child pornography).

Ethical perspectives on pornography

- People agree on some aspects of pornography and censorship, but disagree on others.
- Is pornography, among U.S. adults, legal? Yes.
- Is it moral? Maybe.
- Is its censorship, in the U.S., legal? Yes, it happens on radio and television, and in libraries.
- Is it moral? Maybe.

Analyses concluding that pornography is immoral

- From a Kantian perspective, if the people in pornographic images are being exploited, as a means to a viewer's sexual gratification, then pornography is immoral.
- From a utilitarian perspective, several costs have been identified:
  - It reduces human dignity (i.e., elevation of mind or character).
  - It reduces sympathy for victims of violence or sexual abuse.
  - It causes some people to illegally engage in portrayed behaviors.
  - It offends many people.
  - It diverts resources from better activities.

Analyses concluding that pornography is moral

- From a Kantian perspective, consider if everyone distributed and/or viewed pornography, like they do with vacation photographs. If there is no logical contradiction, then pornography is moral.
- From a utilitarian perspective, considering only pornography among adults, several benefits have been identified:
  - Producers make money.
  - Viewers enjoy it.
  - It is a harmless outlet for sexual fantasies.

Commentary

- Notice the difficulty of performing the utilitarian calculus. People may disagree about whether an aspect of a behavior is a cost or a benefit.
- To summarize, even experts disagree about the morality of pornography among adults.
- In contrast, when children are involved in any way, pornography is generally considered immoral.
- Animated pornography complicates matters further.

Censorship

- *Censorship* is the restriction of public access to content considered offensive or harmful.
- Most censorship is by government or religious institutions.
- The invention of the printing press (ca., 1400s) made censorship more difficult.
- We'll discuss two kinds: direct censorship and self-censorship.

Direct censorship

- A government can monopolize publishers (e.g., newspapers and television stations). For example, copy machines were illegal in the former Soviet Union.
- A government can pass laws regulating publishers. For example, a newspaper cannot publish content compromising national security.
- A government can license publishers. For example, you need a license to broadcast on certain bands of the electromagnetic spectrum. If you violate the rules, you can lose your license.

Self censorship

- A publisher can regulate content for its own reasons. For example, a reporter may refuse to name a source, to improve chances of later information.
- Likewise, a publisher may self-censor information that is critical of a government to help maintain its relationship with that government.
- Publishers can also adopt rating systems for their content. For example, movies, television shows, and video games are rated. Proactive self-censorship can help avoid direct censorship.
- The WWW does not have uniform rating system.

Challenges posed by Internet censorship

- It is decentralized, with point-to-point communication. Anyone can create content.
- It is dynamic. Even the content at a particular URL can change each time it is visited.
- It is huge. Creating a complete up-to-date index is impossible.
- It is global. There is no body of applicable international law.
- Users are anonymous. An adult cannot be distinguished from a child.

Ethical perspectives on censorship (1 of 3)

- Our textbook says that Kant believed censorship was wrong, but it does not explain why, in terms of the categorical imperative.
- What would happen if every government and religious institution prevented public access to incoming and outgoing information they felt was damaging or offensive? Would censorship become unnecessary? Is there a logical contradiction?
- Is the censor using its citizens as a means to an end? Yes, the censor wants to protect itself or (ostensibly) its citizens, rather than treating them as intelligent human beings and allowing them to exercise their own reason and discretion.

Ethical perspectives on censorship (2 of 3)

- According to utilitarianism, censorship has several costs:
  - Since people make mistakes, the prevalent opinion might be wrong, so other opinions should be heard.
  - The truth might be distributed across several opinions, all of which might also contain errors.
  - Even if the prevalent opinion is the truth, comparing it to other opinions tests and validates its truth.
  - An opinion that has been proven true by testing and validation is more likely to influence a person's behavior.
- The main benefit is that damaging or offensive information is not made public.

Ethical perspectives on censorship (3 of 3)

- John Stuart Mill, a founder of utilitarianism, proposed the *Principle of Harm*:

  > The only ground on which intervention is justified is to prevent harm to others; the individual's own good is not a sufficient condition.

  More concretely, a government should let people harm themselves, but not others.
- This helps explain allowing pornography among adults, but censoring child pornography.

Freedom of expression (1 of 3)

- The First Amendment to the U.S. Constitution gives citizens the right to freedom of expression. Its primary purpose is to allow people to openly discuss political issues, but nonpolitcal expression is also covered.
- Previous governments had criminalized such expression as seditious (arousing) or libelous (defamatory), even if true. A person could even be convicted for private communication.
- The medium of expression is not limited to speech. It includes books, magazines, newpapers, radio and television broadcasts, science, art, and certain kinds of conduct (e.g., flag burning and religious ceremonies).

Freedom of expression (2 of 3)

- The U.S. Supreme Court has ruled that freedom of expression is not an absolute right. Protection is not given to:
  libel [written], reckless or calculated lies, slander [spoken], misrepresentation, perjury, false advertising, obscenity and profanity, solicitation of crime, and personal abuse or "fighting" words
- Some restrictions are justified by citing public benefit. Examples are the ban on television tobacco advertisements and zoning laws for adult bookstores.

Freedom of expression (3 of 3)

- The Internet is a form of broadcast expression. The U.S. Supreme Court writes:

  > Of all forms of communication, it is broadcasting that has received the most limited First Amendment protection.
  >
  > Broadcast media have a uniquely pervasive presence in the lives of all Americans.
  >
  > Broadcasting is uniquely accessible to children, even those too young to read.

  In this way, broadcast expression is very different from bookstore or theater content.

Children and the web (1 of 2)

- We have seen that morality and laws treat children differently than adults. This is difficult on Internet, due to its broadcast nature and because a person's age cannot be determined.
- A *web filter* is a tool that can help solve this problem. It blocks web-browser access to objectionable URLs. It is a special case of a general-purpose network-router mechanism called a *packet filter* or *firewall*.
- Some filters use a *blacklist* containing patterns of objectionable URLs.
- Other filters analyze content, blocking access to URLs that appear objectionable.

Children and the web (2 of 2)

- Neither method is foolproof. Both suffer from false positives and negatives. For example:
  - A group can blacklist its enemies.
  - Objectionable sites are created everyday.
  - Science or social-activist sites might contain "objectionable" words.
  - Images are difficult to analyze.

CIPA of 2000 (1 of 4)

- The U.S. Child Internet Protection Act requires libraries using federal money for Internet access to prevent:
  - adults and children from viewing obscenity and child pornography
  - children from viewing harmful content (e.g., pornography)
- Only images must be blocked, not text.
- An adult can ask a librarian to disable the blocking mechanism for access to legal content (e.g., pornography).
- Curiously, obscenity and child pornography were already illegal, and harmful content is poorly defined.

CIPA of 2000 (2 of 4)

- The CIPA refers to the existing federal definition of obscenity, of which there is none. Without a statutory definition, courts will likely apply the Miller obscenity test, from 1973, which defers to state law:
  - An average person applying contemporary community standards must find that the work appeals to the prurient interest (i.e., the work must "turn you on").
  - The work must depict, in a patently offensive way, sexual conduct specifically defined by state law (i.e., the work must "gross you out").
  - The work must lack serious literary, artistic, political, or scientific value (i.e., works with serious value may not be considered obscene).

CIPA of 2000 (3 of 4)

- Most pornography is not legally obscene. Note that to be obscene, the viewer must be turned on and grossed out at the same time.
- Two previous laws, the Communications Decency Act (CDA) and the Child Online Protection Act (COPA), had been successfully challenged, in the Supreme Court, on First Amendment grounds.
- In 2003, the American Library Association sued, in the Supreme Court, claiming CIPA prevents access to inoffensive pages. Further, requiring an adult patron to ask a librarian for freer access was disruptive and stigmatizing. The law was upheld.

CIPA of 2000 (4 of 4)

The Chief Justice wrote:

> A public library does not acquire Internet terminals in order to create a public forum for web publishers to express themselves, any more than it collects books in order to provide a public forum for the authors of books to speak ... Most libraries already exclude pornography from their print collections because they deem it inappropriate for inclusion.

Ethical evaluations of CIPA (1 of 4)

- For a Kantian analysis, if CIPA applied to all computers, not just those in libraries, it would be simple censorship.
- Also, consider that the filters are intended to prevent children from accessing offensive content, but they inadvertently block inoffensive content. The publishers and viewers of that inoffensive content are being used as a means to the end.
- CIPA is immoral.

Ethical evaluations of CIPA (2 of 4)

- For an act-utilitarian analysis:
  - Filtering prevents some children from viewing some offensive content (happy).
  - Some inoffensive content is blocked (sad).
  - Some adults have to ask for filters to be disabled (sad).
  - Some blocking violates the publishers' right to freedom of expression (sad).

  Unfortunately, calculating actual costs and benefits, to determine morality, requires personal judgement. The attributes (e.g., intensity, duration, and certainty) we considered earlier can help.

Ethical evaluations of CIPA (3 of 4)

- According to social contract theory, CIPA must be collectively acceptable to society, because of its societal benefits.
  Apparently, private viewing of offensive content is acceptable, while blocking private access to inoffensive content is unacceptable. Is there a difference if it happens in a public library?
- For some adults, a library provides the only access to the Internet. If they are to be treated as equal citizens, they should have the same access as citizens with private access. They should not have to ask a librarian to disable a filter.
- Social contract theory says we have rules and enforcement so people can create and keep value. Library web filters are not required for this.

Ethical evaluations of CIPA (4 of 4)

- Again, CIPA is immoral.
- Consider virtue ethics. It applies to individual behaviors, not public policy. We cannot use it to determine if CIPA is moral.

Identity Theft (1 of 2)

- About a million people in the U.S. suffered computer-related identity theft in 2005. Now, about 15 million people a year are victims, costing $50 billion.
- An individual can be a victim of *phishing*: the process of sending an official-looking email containing fraudulent instructions. Typically, the instructions try to trick the recipient into browsing an official-looking URL that gathers identity information (e.g., a password or credit-card number).
- A group of people, sometimes a huge group, can be victimized by database theft. Often, this occurs when someone's laptop is lost or stolen. Often, the data should not have been on the laptop's disk in the first place. Disk encryption can mitigate this problem.

Identity Theft (2 of 2)

- On February 21, 2014, the University of Maryland was hacked: 309,000 SSNs of staff, students, and alumni were swiped. The usual solution: Experian lands a contract to provide a year's credit-checking services (309K*$16/mo*12mo: $6M).
- You might think victims are only the elderly or inexperienced. However, the average age of a victim is 40. Often, they are too experienced at providing identity information to web pages.

Chat-room predators

- *Instant messaging* is like email without latency. Estimates suggest that over a billion people use it.
- A *chat room* is instant messaging among multiple people.
- Many people, especially young people, use instant messaging and chat rooms as a replacement for the telephone.
- Pedophiles use chat rooms, lie about their personal characteristics, and try to lure children into physical meetings.
- This is so prevalent that police sting operations use chat rooms to lure pedophiles into physical meetings, for arrest.

Ethical evaluations of police sting operations (1 of 3)

- Here are some utilitarian costs and benefits:
  - The freedom of each convicted criminal is reduced (sad).
  - The safety of noncriminals is increased (happy).
  - People are deterred from criminal behavior (happy).
  - People may have less trust in police (sad).
  - People may have more/less trust in chat-room participants (happy/sad).

  Stings are probably moral.

Ethical evaluations of police sting operations (2 of 3)

- Here's a Kantian perspective:
  - If all, or too many, of the chat-room partipants were police, people would stop using chat rooms.
  - The goal (end) of the police is to convict chat-room criminals. The police use all chat-room partipants as a means to that end, rather than treating them like human beings.

  Stings are immoral.

Ethical evaluations of police sting operations (3 of 3)

- Here's a social contract perspective. Society has agreed to three relevant rules, which the police must enforce:
  - A person should not abuse a child.
  - A person should not misrepresent his/her identity.
  - A person has a right to privacy, including private communication.

  A criminal breaks all of the rules. The police break two of the rules. There is a conflict.
- To summarize, a consequentialist is more likely to consider stings moral.

False information (1 of 2)

- By now, you have all discovered that information on the web must be evaluated for accuracy. How do we know what is true?
- With traditional media, some outlets have earned a reputation for honesty and accuracy, other outlets have a reputation for the opposite. One way to earn a good reputation is to subject content to external review.
- Most web pages are not reviewed directly, except perhaps by the author.

False information (2 of 2)

- However, a search engine can measure a level of indirect review, by associating popularity with accuracy.
- Suppose there are two web pages, A and B. If the number of other pages that link to A is larger than the number of pages that link to B, a search engine can assume that A will be more valuable to a person performing a search, perhaps because A contains better information.
- This is the basis for *page-rank* algorithms, which order the results of a search.

Internet addiction (1 of 4)

- *Addiction* is the persistent compulsive use of a substance, despite its harmful consequences.
- Some psychologists and psychiatrists extend this definition to behaviors, rather than just substances.
- Using a computer for long periods of time can have physical and psychological consequences.
- Of course, there is a test to help determine addiction. One of the eight questions is:

  > Do you feel preoccupied with the Internet (think about previous online activity or anticipate next online session)?

  Five or more affirmative answers indicates addiction. Other experts disagree about the test's value.

Internet addiction (2 of 4)

- Regardless, you can probably agree that a person can use a computer as a way to temporarily escape from the "real" world, and that overuse of this mechanism is unhealthy.
- The psychological traits that make a person susceptible to such addiction seem to be similar to those leading to substance addiction (e.g., stress).
- A person tends to become addicted to a single application.
- Is this sort of addiction immoral? Our textbook considers this question from the perspectives of Kantianism, utilitarianism, and social contract theory. However, it does not use the guidelines developed in Chapter 2.

Internet addiction (3 of 4)

- For Kantianism, what if everyone was addicted? You could argue that no productive work would occur, the Internet would cease to exist, and there would be nothing to become addicted to. Is an addict using a person as a means to an end? You could argue that the addict's family and friends are being used to support the addiction. These arguments seem weak.
- For utilitarianism:
  - The addict finds escape (happy).
  - The addict's health declines (sad).
  - The addict wastes resources (sad).
  - The addict harms other people (e.g., family and friends), via detachment (sad).

  This suggests immorality.

Internet addiction (4 of 4)

- For social contract theory, a rule prohibiting addiction would probably be collectively acceptable to the society, because of its societal benefits. Again, this indicates the immorality of addiction.
- For virtue ethics, addiction does not contribute to personal excellence and reaching one's highest potential. Again, it's immoral.
- In 2013, Chinese authorities announced a plan to develop its own criteria for diagnosing Internet addiction in kids, in the hope of reducing the growing trend. In the plan, they will define the addiction, and spend about three years developing effective methods to intervene in minor online-gaming addictions. Regulations on Internet cafes and online-game companies will become stricter, and a stronger supervision system will be implemented. [China Daily]

Chapter 4: Intellectual Property

- Digital computers allow data to be easily copied. Content includes images, movies, music, databases, and programs.
- In this chapter, we consider:
  - whether such intangible content is property
  - whether an author has rights to control its reproduction
  - what mechanisms have been created to protect these rights

Intellectual property rights

- *Intellectual property* (IP) is any unique product of the human intellect with commercial value (e.g., the content listed earlier, paper-printed content, inventions, and chemical formulas).
- The property is the content, not the delivery mechanism (e.g., for a novel, the property is the story, not the printed pages). You can buy a DVD, but the movie is the property of someone else.

Right to property (1 of 2)

- The idea of a natural right to property was developed by the English philosopher John Locke (1632-1704), who wrote:
  - People have a right to property in their own person. Nobody has a right to the person of anybody else.
  - People have a right to their own labor. A person should benefit from their own work.
  - People have a right to things they have removed from nature through their own labor.

Right to property (2 of 2)

- This explains how a person can develop a home on a parcel of land in the wilderness and then claim to own it.
- To Locke, this makes sense as long as two conditions hold:
  - No one claims more than they can use.
  - When someone removes something from the common state, there is plenty left for others.
- Of course, this reasoning only applies to unlimited resources.

Locke and IP (1 of 2)

- Can Locke's physical-property reasoning be extended to IP? We can try, but it leads to paradoxes:
  - If two people independently develop the same IP (e.g., a musical composition or an invention), there is actually only one ownable object. Both cannot have full ownership of a single object.
  - If one person develops an IP object, and another person "steals" a copy, the developer still owns the object, albeit nonexclusively. Further, the developer could have prevented the "theft" by keeping the development a secret.

Locke and IP (2 of 2)

- The paradoxes are due to these facts:
  - Every IP object is unique: two identical objects are really the same object.
  - Copying an IP object is different than stealing a physical object.

IP and society (1 of 3)

- The results of creative activities can greatly benefit members of a society.
- Some people want to freely share their creations; others are less altruistic and expect more personal benefits.
- Ben Franklin, for example, was a prolific inventor, but patented none of his inventions.
- Therefore, even if there is no natural right to IP, granting such a right can have beneficial consequences.
- Recognizing this, the U.S. Constitution gives Congress the power to grant IP rights to authors and inventors.

IP and society (2 of 3)

- A person can make money from IP in at least three ways:
  - With exclusive access to the IP, the holder can distribute artifacts to the public without competition.
  - The holder can license the IP to another party, who distributes artifacts to the public without competition.
  - The holder can license the IP to another party, who prevents distribution to avoid competition with other IP.

IP and society (3 of 3)

- Society benefits from free use of IP, but granting IP rights increases innovation.
- Congress addressed this dilemma by compromise: IP rights expire after a certain amount of time, depending on the type of IP.

IP protection

- In the U.S., IP can be protected in one of four ways:
  - as a trade secret
  - by patent
  - by copyright
  - as a trademark (or servicemark)

Trade secrets

- A *trade secret* is a confidential piece of IP providing a company with a competitive advantage (e.g., a formula, process, or design).
- The company must actively try to keep it secret. For example, an employee must sign a confidentiality agreement.
- A trade secret is not registered, and does not expire.
- Another company can legally "reverse engineer" a trade secret. If you can guess the recipe for Coca-Cola, you are free to market a drink that tastes the same.

Trademarks and servicemarks

- A *trademark* is a word, symbol, picture, sound, color, or smell used by a company to identify a product.
- A *servicemark* identifies a service.
- They allow a company to establish a "brand name."
- A company tries to avoid having its brand name used as a common noun.
- A trademark need not be registered, and does not expire.

Patents

- A *patent* grants an inventor exclusive rights to a novel piece of IP.
- The IP is not confidential. Indeed, a patent is a public description of the IP.
- Patents are maintained by the government, which also determines novelty.
- A patent expires after 20 years.

Copyrights (1 of 4)

- A *copyright* provides an author certain rights to an original written work.
- A copyright holder has these rights:
  - reproduction
  - distribution
  - public display
  - public performance
  - derivation of new works

Copyrights (2 of 4)

- A copyright holder can prevent others from exercising these rights, and they can charge others to exercise these rights.
- In the U.S., in 2013, this accounts for over $1 trillion annually, 6.5% of the gross domestic product.
- Copyright industries accounted for $142 billion in foreign sales and exports, far more than aerospace, agriculture, food, pharmaceuticals, and medicines.

Copyrights (3 of 4)

- Works created before 1978 are protected for 95 years.
- Later works are protected for 70 years after the author's death.
- If the work is made for hire, it is protected for 95 years from the date of publication or 120 years from the date of creation, whichever is less.
- Since 1958, Congress has extended the length of protection 11 times.

Copyrights (4 of 4)

- In 1991, Kinko's Graphics was successfully sued for $510,000 for selling "class notes" to college students, copied from chapters of copyrighted books.
- In 1994, a bulletin board system (BBS) operator was sentenced to six months of home confinement, and subsequent probation, for posting copyrighted software. His customers paid $99 a year for access.
- Also in 1994, an MIT student ran a similar BBS, but was acquitted because he did not charge for access.
- In 1997, Congress passed a law that made such reproduction or distribution illegal, regardless of profit.

Fair use (1 of 6)

- The IP rights granted to a copyright holder are limited.
- A copyrighted work can be copied under circumstances known as *fair use*. These include short excerpts for:
  - research
  - criticism
  - commentary
  - news reporting

Fair use (2 of 6)

- Four factors must be considered:
  - What is the purpose and character of the use? Is it educational or commercial? Educational is better.
  - What is the nature of the work being copied? Is it nonfiction or fiction? Is it published or nonpublished? Nonfiction nonpublished is better.
  - How much of the work is being copied? Is it a paragraph or a chapter? An excerpt is better.
  - How will this use affect the market for the work? Is it out of print or available? Is the use spontaneous or scheduled? A spontaneous copy of unavailable material is better.

Fair use (3 of 6)

- Consider the Kinko's case.
- Kinko's profited from the packets of copies of copyrighted material.
- Depending on the course, the material may have been nonfiction or fiction.
- Entire chapters of typically in-print books were included.
- The packets were created before the course started, allowing students to avoid buying the books.
- This is not fair use.

Fair use (4 of 6)

- Consider a professor who scans copyrighted journal articles and posts them on a password-protected website for a class.
- The use is educational.
- The work is published nonfiction.
- Only particular articles in a journal are scanned.
- They are also available in the library, so the market is not affected.
- This is fair use.

Fair use (5 of 6)

- Consider an art professor who lectures with slides made from copyrighted photographs of noncopyrighted paintings in a book.
- The use is educational.
- The work is published fiction.
- Only particular photographs in the book are used, but each photograph is used in its entirety.
- Unless the book's publisher sells slides of the photographs, the market is unaffected.
- This is fair use.

Fair use (6 of 6)

- Consider personal videotaping of a copyrighted television show or movie, for later viewing.
- The use is not commercial.
- The work is published nonfiction or fiction.
- A work is copied in its entirety.
- The market is affected if a viewer skips advertising, but there may be more viewers.
- In 1976, the Supreme Court ruled that this was fair use. Note well that the defendant was Sony, an equipment manufacturer, not a viewer. The ruling also recognized that such equipment could record noncopyrighted material, too.

More copying (1 of 7)

- Consumer videotape recording was like early audiotape recording: analog. The first copy was moderately acceptable, but a copy of a copy was of poor quality. This limited illegal copying.
- Of course, digital technology produces perfect copies. Copying became more of a problem as digital audio tape and writable CDs and DVDs became consumer products.
- The Audio Home Recording Act of 1992 allows consumers to make personal copies.
- It also requires manufacturers of digital recording gear to employ a technology that prevents making a copy of a copy.
- Furthermore, artists and recording companies are paid a royalty on sales of digital gear.

More copying (2 of 7)

- In 1998, a manufacturer of MP3 players was sued, because they omitted the copy-a-copy technology.
- MP3 is a lossy compression algorithm: its output is much smaller than its input, and some data is lost.
- The manufacturer won, because the MP3 file came from a computer's hard disk and was not an exact copy of the original digital work.
- Even creating the MP3 file on the computer was legal, because it wasn't an exact copy.
- A computer does not need the copy-a-copy technology, because it is not primarily a digital recording device.

More copying (3 of 7)

- Illegal digital copying is big business.
- Recording companies have given up trying to stop copying. Now, they just want to stop distribution.
- In 1998, the Digital Millennium Copyright Act (DMCA) revised U.S. copyright law:
  - It significantly reduces fair use.
  - It criminalizes the circumvention of encryption on digital media and the sale or even discussion of software to do so.
  - ISPs can be sued if they do not try to help enforce the law.

More copying (4 of 7)

- The application of copy-protection schemes or encryption, to protect copyrights, is called *digital rights management* (DRM).
- In 1999, about 200 companies formed the Secure Digital Music Initiative (SDMI). They wanted to develop DRM technology to "watermark" media.
- In 2000, they offered $10,000 to anyone who could "hack" the scheme.
- A Princeton professor did, refused the prize, and tried to publish his results. He was threatened with a DMCA lawsuit and withdrew the paper. It leaked, anyway, and was later published.

More copying (5 of 7)

- Even before that, many of the SDMI companies lost interest. They found they could make more money selling devices that played illegally copied media.
- Sometimes, DRM backfires.
- In 2005, Sony sold audio CDs with copy protection that installed software on Windows PCs that played them. The installed software had a security vulnerability, allowing administrative privileges (i.e., a rootkit). Sony was sued and had to undo all the damage.

More copying (5 of 7)

- After CDs, recording companies saw a second chance in protecting DVDs (believe it or not: Digital Versatile Disc).
- The encryption scheme was called Content Scramble System (CSS). DVD players and drives contain a licensed copy of CSS software and decryption keys.
- In 1999, a teenager from Norway wrote a program that decrypted CSS-encrypted media.
- He distributed his program on the Internet. A magazine published it.
- The magazine was sued in the U.S. for violating the DMCA. It claimed the program was free speech and protected. The court said the program was more "functional" than "expressive" and its potential to do harm limited its protection. The magazine lost.
- The teenager was sued in Norway, and was acquitted.

More copying (6 of 7)

- After DVDs, recording companies saw a third chance in protecting high-definition DVDs (HD-DVDs), with the Advanced Access Content System (AACS).
- In 2007, someone posted the AACS encryption key at `digg.com`, a social news site.
- AACS representatives contacted Digg. Digg cooperated, essentially due to fear.
- Digg users were outraged and posted the key across the Internet.
- Eventually, Digg reversed its decision and supported its users.
- The key was "expired," but the new key was eventually posted, too.

More copying (7 of 7)

- Some recording companies are still trying to make copyproof CDs.
- One technique takes advantage of a difference between audio players and computer CD drives. Since audio players skip over errors, a CD with intentional errors cannot be read by a computer CD drive and conventional software.
- However, special software can skip the errors (e.g., `cdparanoia`).

Criticisms of DRM

- There are several criticisms of DRM:
  - Technological schemes do not seem to work, for long.
  - It prevents fair use (e.g., for a library).
  - It never expires.
  - Some schemes infringe on privacy (e.g., they "phone home").

Apple DRM

- Apple's music DRM scheme is called FairPlay.
- It only works on Apple hardware (running QuickTime), which can be seen as monopolistic.
- Apple's key servers know which registered devices you own.
- Replying to requests to license FairPlay to other vendors, Steve Jobs said doing so would leak the trade secret to hackers.
- Instead, Apple decided to offer DRM-free versions of music at a slightly higher price.

Peer-to-peer networks (1 of 3)

- The most common network-application architecture is a client/server arrangement. For example, a web browser is a client of a web server. Multiple clients share a server.
- A more distributed architecture is a *peer-to-peer* arrangement, where any node can act as a client or server.
- In a file-transfer application, any node can provide files to any other node. There is no centralized control or bottleneck, except (perhaps) for indices. Examples are Napster, KaZaA, Grokster, Morpheus, and BitTorrent.

Peer-to-peer networks (2 of 3)

- Needless to say, recording companies do not like peer-to-peer networks.
- They have tried to sue groups of individuals under the DMCA.
- They have also tried to flood the illegal market with spoofed MP3 files: music files that contain garbage. One claim is that such spoofs are downloaded 200 million times a month.
- Universities are hotbeds of music file sharing. They have fast networks and big disks. In 2003, four students at three universities were sued for $100 billion for sharing between 27 thousand and 1 million songs. They settled for several thousand dollars apiece.

Peer-to-peer networks (3 of 3)

- In 2003, MGM (and others) sued Grokster for promoting illegal copying among its users. A U.S. District Court dismissed the suit without a trial. The court compared Grokster to a VCR manufacturer (e.g., Sony).
- MGM appealed and lost, again.
- MGM then appealed to the U.S. Supreme Court and won, unanimously! The court ruled that a supplier of technology that can violate copyrights is liable for the violation. Sony was different: a VCR lets a person watch a show later, rather than promoting copying and distribution.

Protections for software (1 of 6)

- Is software IP? If so, what kind of protection applies?
- Trade secret? Trademark?
- You cannot patent a mathematical formula, so patents do not seem right for algorithms.
- A copyright protects the expression of an idea, not the idea itself. You can copyright an implementation (e.g., the source and/or object code, and the screen display), but not the concept of what the implementation does.

Protections for software (2 of 6)

- Prior to 1960, most commercial software was bundled and licensed with hardware.
- In 1964, people started copyrighting software. You could register a program with the Copyright Office.
- The Copyright Act of 1976 explicitly recognizes that software can be copyrighted.
- The definition of copying a program is broad. Indeed, installing a program or even running a program copies it. Of course, license agreements allow this. These are violations:
  - copying to a CD for resale
  - copying to a hard disk for resale of the computer
  - Internet distribution

Protections for software (3 of 6)

- Companies can violate copyrights, too.
- In the early 1980s, Apple sued Franklin Computer for copying a ROM, and won.
- In 1992, Sega sued Accolade for disassembling the object code of a video game to determine a proprietary hardware interface, and lost.

Protections for software (4 of 6)

- In 1981, a U.S. Supreme Court decision forced the Patent and Trademark Office (PTO) to consider software patents.
- The PTO had to differentiate algorithms from inventions. Is an algorithm discovered or invented?
- The PTO tried to differentiate by considering the data manipulated by the software. If they are just abstract "values" a patent is inappropriate. If they are real-world "measurements" a patent is more appropriate. Does this seem reasonable?

Protections for software (5 of 6)

- Another problem was determining novelty.
- The PTO compares a patent application to *prior art*: existing patents.
- Of course, in 1981, there was no prior art. Any application was novel. This led to truly ridiculous patents. It still does.
- Some people filed very broad patents, just so they could later sue legitimate developers for patent violation. They are called *patent trolls*.

Protections for software (6 of 6)

- Accidental and/or inadvertent violation of software copyrights is common.
- Developers move from company to company, taking their brain, full of IP, with them.
- Using "free" software in a commercial product can violate its copyright.
- There is tension between IP and compatibility.
- The textbook describes using one team to analyze a competitor's product to develop a specification, and another team to use the specification to develop a compatible product. Since the second team never sees the original IP, they cannot have violated the protection.

Open-source software (1 of 4)

- Originally, companies (e.g., IBM) distributed source and object code with the hardware they sold or licensed to their customers.
- In the 1970s, companies started treating source code as a trade secret, distributing only object code. They stopped selling software. Instead, they sold licenses, allowing their customers to execute programs.

Open-source software (2 of 4)

- Governments grant IP protection to software for perceived beneficial consequences: increased innovation that benefits society.
- Harmful consequences have also been identified. These are from Richard Stallman:

  `pub/ch4/rms`
- The *open-source movement* is a philosophy that software should be freely distributed. It has these characteristics:

  `pub/ch4/opensource`
- Note that there is no restriction against selling open-source software.
- There are nearly a hundred different open-source licenses.

Open-source software (3 of 4)

- Several beneficial consequences of open-source software have been identified:

  pub/ch4/os-benefits
- The Internet's infrastructure depends on open-source software:

  pub/ch4/os-examples
- Surveys indicate that the quality and dependability of open-source software is about the same as that of commercial software.
- The popularity of open-source software is at least partially due to early successes:

  pub/ch4/os-early

Open-source software (4 of 4)

- In 2007, Linux's share of the server market was estimated at 12.7%. A 2008 estimate suggested that 60% of all web servers ran Linux. Linux has only about 2% of the desktop market.
- You'll hear the following criticisms of open-source software:

  pub/ch4/os-criticism

Legitimacy of IP protection for software (1 of 4)

- When you accept a license to use proprietary software, you usually agree not to sell or give it to other people. If you redistribute it you are violating the law.
- Is it moral for a society or its government to grant IP protection to software?
- From a social-contract perspective, the author of a program has a right to own it. Programming is hard work, a hard-working author should be rewarded with the result of the work, ownership implies control, and a government enforces ownership. This suggests protection is moral.
- However, the argument is weak because it is based on tangible-property rights, They fail to recognize that making a copy differs from taking the original away from the author.

Legitimacy of IP protection for software (2 of 4)

- From a utilitarian perspective, these are consequences of granting IP protection:
  - The author profits from sales (happy).
  - Some of the author's profits will be used to develop new programs for customers (happy).
  - A customer cannot redistribute programs (sad).
- Again, this suggests protection is moral.

Legitimacy of IP protection for software (3 of 4)

- However, the argument utilitarian is again weak:
  - Preventing an illegal copy does not always increase sales. The copy might go to someone that would never buy the program. Also, illegal copies might be a kind of publicity that increases sales.
  - Reduced sales of software does not guarantee reduced development of new software. Microsoft is a victim of illegal copying, but they are quite successful. In contrast, open-source developers keep producing new software, without any sales.

Legitimacy of IP protection for software (4 of 4)

  - Software production is not completely driven by sales to customers. Hardware vendors (e.g., Intel) encourage development of complex programs, so users need to upgrade their hardware.
  - Not all new software is necessarily good for society.
- We conclude that the arguments for IP protection of software are not strong.

Creative Commons

- One of the problems with copyright law is that an original work is implicitly and automatically protected, even if the author would like to share it. It discourages collaboration.
- Creative Commons is a nonprofit corporation that provides standard copyright-license forms for free. An author can fill-out a form, retain the copyright, but allow others to use the IP in certain ways. Since Creative Commons maintains the license, someone who wants to use the IP does not have to contact the author to ask permission.
- A license can permit these uses:

  pub/ch4/os-cc
- By 2005, more than 10 million pieces of IP had been distributed using Creative Commons.

Chapter 5: Privacy

- In this chapter, we try to define privacy and decide whether we have a right to it. Is it like our rights to property and liberty? It's not mentioned in the U.S. Constitution or Bill of Rights. It can conflict with our right to free expression.
- We then consider how technology allows "personal" information to be gathered and analyzed. Several laws have been passed to promote/control such gathering and analysis. We'll consider how effective they are.
- Identity theft has become a common crime. We'll discuss how it happens, and how social security numbers have become personal identifiers. We'll consider national identification cards.
- Finally, we'll see how encryption can provide privacy, and how governments try to control encryption technology.

Perspectives on privacy (1 of 7)

- *Privacy* is a social arrangement that allows individuals to have some level of control over who is able to gain access to their physical selves and their personal information.
- Too much privacy can be harmful:
  - Illegal or immoral activities are often performed privately.
  - A community can ignore its members' needs in the name of privacy (e.g., a family's poverty or violence).

Perspectives on privacy (2 of 7)

- Privacy has many benefits:
  - It is how society recognizes a person as an adult, and lets them be responsible for their own behavior.
  - It allows individuals to develop and be themselves.
  - It lets people shut out the world, be creative, and develop spiritually.
  - It lets a person develop different kinds of relationships with different people.
- Most believe that allowing people at least some privacy is better than denying them any privacy.

Perspectives on privacy (3 of 7)

- Our belief in a right to privacy evolved from property rights. European tradition established a person's home as his/her sanctuary. Not even the King could enter without permission. The Third and Fourth Amendments, in the U.S. Bill of Rights, are about this (e.g., quartering of troops and being secure in your house).
- In 1890, Warren and Brandeis published a paper called "The Right to Privacy," which described the "right to be let alone," especially by newspapers.
- In summary, people disagree about whether privacy is a natural right, but most agree that society benefits from some privacy rights.

Perspectives on privacy (4 of 7)

- An example of protecting privacy rights is the U.S. "Do Not Call Registry." The number of Americans who felt that it was "extremely important" not to be disturbed at home jumped from 49% in 1994 to 62% in 2003. Fifty million phone numbers were placed in the register, before it even started, in 2003.
- Many technological advances have increased our privacy: single-family homes, cars, televisions, and computers. We can do what we do without being among other people.

Perspectives on privacy (5 of 7)

- Privacy-related activities can be categorized:
  - *Information collection*: The trail of data you leave behind can be recorded (e.g., activity/transaction logs and camera footage).
  - *Information processing*: Collected data can be analyzed and aggregated.
  - *Information dissemination*: Collected data can be distributed, accidently or intentionally, or even sold.
  - *Invasion*: A person's activities can be intruded upon, interrupted, or interferred with (e.g., spam).

Perspectives on privacy (6 of 7)

- Here's an example from the textbook. A couple buys software that allows them to use their computer to monitor, via live video, the nanny caring for their child. The nanny does not know about it. Is the couple's behavior moral?
- For act utilitarianism:
  - The monitoring is expensive (sad).
  - The parents will probably be reassured of good care (happy).
  - If the (good) nanny finds out, she may quit (sad/sad).
  - If the nanny is abusive, she'll be fired (happy/sad).

  Probabilities are needed.

Perspectives on privacy (7 of 7)

- For rule utilitarianism, if monitoring was common enough that nannies expected it:
  - A nanny would not expect the privacy to be abusive (happy).
  - A nanny's job would be less pleasant (sad).
  - The overall quality of nannies might go up/down (happy/sad).

  Again, hard to say.
- For social contract theory: secretly monitoring the nanny violated her right to privacy. It's immoral.
- For Kantianism: If every parent "secretly" monitored their nanny, it would not be secret anymore. Also, the nanny is certainly being used to relieve the parent's concern.

Information disclosures (1 of 2)

- As we live our lives, we leave a trail of information. Some is part of the public record (e.g., birth certificates). Some is held privately (e.g., commercial transactions and website access).
- Here are some other examples.
- Facebook photo tags: Your name and image are connected.
- Cell-phone 911 enhanced services: Your location is tracked, within 100 meters.
- Rewards or loyalty programs: Your purchases are recorded.
- Body scanners (not for security): Your measurements are recorded.
- Radio-frequency identification (RFID) tags: Embedded in products, they indicate your location within 6 feet.
- Implanted RFID chips: They allow pet, medical condition, and child identification. They can be debit cards, too.

Information disclosures (2 of 2)

- OnStar: It allows car monitoring, location tracking, and remote control (e.g., disable gas pedal).
- Car black boxes: In modern cars, data is collected and stored for the 5 seconds before airbag deployment.
- Medical records: They might be stored in a centralized database, suitable for mining (e.g., by insurers or employers).
- Digital video recorders (DVRs): They record your viewing habits and ad-skipping behavior (i.e., 66% for broadcast networks during primetime).
- Cookies and Flash cookies: These hold client-side website state. Flash cookies are not affected by browser privacy settings.

Data mining (1 of 3)

- Some companies buy and sell personal information.
- *Data mining* is the process of refining and/or integrating data from multiple sources.
- For example, combining your location and buying habits can produce localized advertising. Likewise, it can be used to make recommendations for products (e.g., a movie).
- Does a company have a right to sell information about their customers' transactions, or should the person have the right to control that information?

Data mining (2 of 3)

- Example from the textbook: Suppose a computer-science professor cannot fix his broken computer, so he takes it to a computer shop, which takes three weeks to diagnose and fix the problem. The professor wants to keep the transaction private, to avoid the embarassment of not being able to fix the computer himself. The shopkeeper wants the same, but to avoid the embarassment of the repair taking so long. In this case, both parties want the same thing. But, in general, who has the right to decide.
- There are two different policies: opt-in and opt-out.

Data mining (3 of 3)

- With *opt-in* the consumer must explicitly give permission for the organization to share information. It's preferred by privacy advocates.
- With *opt-out*, the consumer must explicitly forbid the organization from sharing. It's preferred by direct-marketing groups. It's far more common.

Examples of data mining

- *Credit reports* are a great example. A person's financial data is gathered from multiple sources, aggregated, and sold to other companies.
  A good credit report simplifies getting a loan. Bad report entries do the opposite, and are often retained for seven years. Mistakes can be hard to fix, too.
- *Microtargeting* gathers a person's political data, to personalize voting or donation solicitation.
- Assembling a person's *information mosaic* can produce surprising results. The textbook mentions aggregating (essentially a database join) tollbooth-transponder and credit-card information, and selling it to a bank, to target frequent drivers with car-loan advertising.

Organizations push the boundaries (1 of 2)

- The cost of data mining is dropping, while the value of data is increasing. Protecting privacy is becoming more difficult.
- Here are some examples.
- In 1990, Lotus Development Company developed a CD, for sale, containing data on 120 million people, including income from the credit bureau Equifax.
- In 2007, Facebook started an opt-out service that would tell your "friends" about your online purchases.

Organizations push the boundaries (2 of 2)

- In 2006, Netflix offered a prize for a better movie-recommendation algorithm. To help contestants, they released over 100 million "anonymized" ratings. The person rating the movie was an anonymous integer. However, researchers demonstrated that combining this with other data could identify the person rating a movie, which reveals potentially sensitive information about them.

Examples of consumer backlash (1 of 4)

- The cost of acquiring consumer information continues to drop, while its value continues to rise.
- These incentives put pressure on individual privacy. How can individuals fight back?
- Recall that Lotus and Equifax developed a database on 120 million people, and were preparing to sell it, as "Marketplace: Households." It included household income. In 1991, the plan was cancelled, due to massive protests, 30,000 complaint letters, and threatened lawsuits. They dropped the project.

Examples of consumer backlash (2 of 4)

- Sadly, Acxiom and the credit bureau, Experian, are selling even *more* detailed databases, today. They have records on 500 million people, with an average of 1500 pieces of data per person.
- Other companies do this, too. For example, you can buy lists targeted to particular health conditions (e.g., bipolar disorder).

Examples of consumer backlash (3 of 4)

- Recall that Facebook partnered with several retailers (e.g., eBay), to create "Beacon," to advertise what *you* bought to your "friends." Imagine buying your friend a gift. It was an opt-out policy, which many people discovered too late. In 2007, 50,000 Facebook users joined a group to complain. Zuckerberg apologized, and switched to an opt-in policy.
- In 2011, two malls started tracking their in-store customers, via cell-phone wifi. They were mainly interested in which stores were visited. You could not opt-out. A U.S. senator prompted the malls to stop, after only three days. The senator said, ". . . they can ask your permission to do so."

Examples of consumer backlash (4 of 4)

- In 2012, an iPhone app, named "Path," was found to be uploading the phone's address book, without asking the user. After a storm of complaints, Path apologized, and changed the behavior to be opt-in. Soon after, many apps were found to do this (e.g., Twitter). They changed to opt-in, too.
- In 2012, Facebook's Instagram changed its privacy policy/agreement, allowing Instagram to use, without permission or compensation, customer content in commercial advertising. Responding to the uproar, a cofounder responded that the new policy was misunderstood, but changed it back.

Chapter 6: Privacy and the government

- In this chapter, we consider the impact local, state, and federal governments have on the privacy of people living in the US.
- We look at compromises between individual privacy and government attempts to prevent criminal and terrorist activity.
- We look at government agencies that have broken the law to protect public safety and/or national security.
- We will see that the Supreme Court has, over time, shifted its interpretation of the Constitution, regarding privacy.

A taxonomy of privacy

- As we saw last chapter, privacy-related activities can be categorized:
  - information collection
  - information processing
  - information dissemination
  - invasion
- We begin with a chronology of government collection of citizen data.
- Then, we'll see a chronology of laws, and changes to laws, related to collection of such data.
- Then, we'll discuss processing, storage, and dissemination of such data.
- Finally, we'll consider laws to limit privacy invasion.

Government data-collection history (1 of 11)

- The US Census:
  - 1790: Six simple questions: age, sex, color, free/slave status.
  - 1820: Added employment category.
  - 1840: Added school attendance, literacy, and occupation.
  - 1850: Added taxes, school, crime, wages, and property values.
  - 1940: Added random sampling and many more demographic questions.
  - today: American Community Survey mails fifty questions to 5 million addresses, including questions about ancestry/ethnicity, language, marriage, transportation, and energy/fuels.

Government data-collection history (2 of 11)

- The federal income tax:
  - 1862: Created to help pay for the Civil War.
  - 1872: Repealed.
  - 1894: Reinstated, but ruled unconstitutional a year later.
  - 1913: Made constitutional, by 16th Amendment, enabling prohibition.
  - today: Revenue is more than $2 trillion per year. IRS forms requires many personal/private details: income, assets, expenses, contributions, etc.

Government data-collection history (3 of 11)

- 1967: FBI National Crime Information Center (NCIC). It now has 13 million records in 21 databases, containing data about crimes and investigations.
- 2005: OneDOJ database combines crime/terrorist data from five federal law-enforcement agencies, not available in the NCIC.
- 1968: Closed-circuit TV cameras (CCTV) are used by police to monitor and record pedestrian and transportation activity. Today, there are 30 million in the US. Only a tiny fraction of people recorded are criminals.

Government data-collection history (4 of 11)

- 1980: License-plate scanners use a camera to record license-plate data, date/time, and other data. They are mounted on street posts or police cars. The data is often stored forever. Again, only a tiny fraction of people recorded are lawbreakers.
- 2013: Unmanned aerial vehicles (UAVs) are small drones with video cameras, that can perform surveillance from an altitude of less than 400 feet. They aren't the armed military weapons. Is a search warrant required?

Government data-collection history (5 of 11)

- A government can also gather private data by intercepting private communication:
  - face to face
  - US Mail
  - other physical shipping
  - over wired telephones
  - over wireless telephones/radios
  - over computer networks
- Collectively, we'll call these interception methods wiretaps and bugs.

Government data-collection history (6 of 11)

- 1892: New York makes wiretapping a felony. Until 1920, NYC police ignored the law and intercepted calls.
- 1925: Wiretapping was used to convict Roy Olmstead of bootlegging, in Seattle. He argued that the warrantless privacy violation, by federal agents, was unconstitutional.
- 1928: The Supreme Court upheld the conviction (5-4), saying the 4th Amendment protected only tangible assets. Agents did not "search" a physical place and did not "seize" a physical item.

Government data-collection history (7 of 11)

- This is the 4th Amendment:

  pub/ch6/Amendment4.txt

  This is part of Louis Brandeis' famous dissent, for the Olmstead case:

  pub/ch6/Brandeis.txt

  Does it apply to other media/content?
- 1934: The public and press were critical of the 1928 decision. Congress passed the Federal Communications Act, making disclosure of wiretap content illegal. Three years later, the Supreme Court reversed its position. After four years in prison, Olmstead was pardoned by the president and compensated with money. The FBI announced it would cease warrantless wiretaps.

Government data-collection history (8 of 11)

- 1941: US agencies have access to all telegrams, for censorship.
- 1945: The FBI illegally continues warrantless wiretaps, and presses to have the law changed.
- 1945: Telegram censorship ends, but the NSA (nee, Signal Security Agency) asks the three telegram companies to violate federal law and continue giving them microfilm access to international telegrams, for national security. The operation is called "Shamrock."

Government data-collection history (9 of 11)

- 1960: Shamrock converts from microfilm to electronic access. Content can now be searched, by computer.
- 1961: The NSA develops "watch lists" for monitoring: organized crime, people working with Cuba, Vietnam War protesters (e.g., Joan Baez), and drug traffickers.
- 1967: The Supreme Court rules that a bug, even outside a phone booth, is effectively a wiretap:

  `pub/ch6/Katz.txt`
- 1975: Amid congressional and press scrutiny, Shamrock ends.

Government data-collection history (10 of 11)

- 1997: The FBI's "Omnivore" (Sun Solaris), and then "Carnivore" (Microsoft NT), projects are implemented. Carnivore is an IP packet sniffer, installed at a suspect's ISP, to monitor/record Internet traffic. At first, it was used with a warrant.
- 2000: The FBI demands that Earthlink use Carnivore without a warrant. Earthlink sues, and loses.

Government data-collection history (11 of 11)

- 2002: The CIA obtains telephone numbers of several top al-Qaeda members, and gives them to the NSA. President Bush signs an executive ordering allowing the NSA to intercept outgoing international calls and emails, without a warrant. As many as 500 people were monitored.
- 2003: The DoD creates "TALON," a database of suspicious activities and threats near military bases. It was found to also contain data about antiwar protesters and college students.
- 2007: TALON ends.

Data-collection legislation (1 of 7)

- 1988: The Employee Polygraph Protection Act (EPPA) prohibits private employers from giving lie-detector tests. Exceptions: some drug and security employers, one that has suffered an economic loss, and government employers.
- 2000: The Children's Online Privacy Protection Act (COPPA) requires parental consent before online collection of data from kids twelve and younger.
- 2008: The Genetic Information Nondiscrimination Act prohibits health-insurance companies and employers from using genetic information to make decisions. Exceptions: life-insurance companies and small (< 15) employers.

Government data-collection legislation (2 of 7)

- We saw that the events of 1934 and 1967 made warrantless wiretaps illegal.
- 1968: Title III of the Omnibus Crime Control and Safe Streets Act allows a court-ordered wiretap for up to thirty days.
- However, government agencies want warrantless wiretaps, in cases of national security.
- 1972: The Supreme Court rules that warrantless wiretaps are unconstitutional, even for national security. Remember this!

Government data-collection legislation (3 of 7)

- 1978: The Foreign Intelligence Surveillance Act (FISA) allows the President to authorize warrantless electronic surveillance of foreigners, for up to a year, as long as the communication is not with a US citizen.
- If a US citizen is involved, a warrant from a secret federal FISA Court is required.
- In 2008, the it is amended, to remove the warrant requirement if one end of the communication is outside the US.

Government data-collection legislation (4 of 7)

- 2013: Edward Snowden describes the NSA's "PRISM" program, which provides direct access to servers at: Google, Facebook, Yahoo, Microsoft, Apple, AOL, and others.
- PRISM gives the NSA warrantless access to stored information, when the NSA has reasonable suspicion that the person being investigated is a foreigner outside the US.
- The technology companies didn't even know about it, but the Obama administration confirmed it.

Government data-collection legislation (5 of 7)

- 1986: The Electronic Communications Privacy Act (ECPA) allows a new kind of wiretapping: metadata gathering.
- The device shows incoming and outgoing phone numbers, but does not monitor content. Attaching it requires a warrant, but not probable cause, and approval is virtually automatic.
- The ECPA also allows warrants for "roving" wiretaps, where a suspect's calls can be monitored on any phone.

Government data-collection legislation (6 of 7)

- The Stored Communications Act (SCA), part of the ECPA, allows the warrantless seizure of emails from an ISP, if they are older than 180 days.
- Thus, the privacy of Internet communication is no longer protected by the 4th Amendment.
- The SCA still requires a warrant for newer email.
- 2010: Federal prosecutors demand that Yahoo provide newer already-read emails, without a warrant.
- Yahoo, backed by Google and others, challenged the order. The government withdrew its request.

Government data-collection legislation (7 of 7)

- Analog phones are easier to wiretap than digital phones (e.g., voice over IP (VoIP).
- 1994: The Communications Assistance for Law Enforcement Act (CALEA) requires phone-network equipment to allow the FBI to conduct warranted wiretapping.
- The FBI wanted not only metadata and content, but mid-call keystrokes (e.g., passwords) and other data.
- 1999: The FCC issues the CALEA guidelines.
- 2005: The FCC includes VoIP and broadband protocols.

USA Patriot Act (1 of 11)

- 2001: In response to the World Trade Center and Pentagon attacks, Congress passes the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT).
- It changed many existing laws:
  - It gave US agencies more authority to monitor communications.
  - It gave the US Treasury more authority to prevent foreign money laundering.
  - It tried to prevent terrorists from entering the US.
  - It defined new crimes and penalties for terrorist activity.

USA Patriot Act (2 of 11)

- It expands the use of ECPA metadata-gathering devices to networks, tracking email addresses and URLs. As before, probable cause is not needed and warrant approval is virtually automatic.
- The approving judge need not have jurisdiction over the surveillance location.
- It expands the use of roving wiretaps, from law enforcement to intelligence gathering. No proof is needed that the monitored equipment is even used by the suspect. The authorizing judge gets no feedback about the warrant.

USA Patriot Act (3 of 11)

- It authorizes a warrantless search/seizure when there is "... reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse effect."
- It authorizes a warrantless seizure of property that "... constitutes evidence of a criminal offense in violation of the laws of the US," even if unrelated to terrorism.
- Thus, the security of a citizen's "person, house, papers, and effects" is no longer protected by the 4th Amendment.

USA Patriot Act (4 of 11)

- It expands the use of a procedure, from the ECPA, called a National Security Letter (NSL).
- The FBI can issue a NSL, to obtain a search warrant, without showing probable cause and without a judge's approval.
- The recipient of an NSL cannot disclose receipt (i.e., there's a "gag" order, built in).
- The FBI can then collect Internet, business, medical, educational, library, and religious records.
- From 2003 to 2006, the FBI issued 192,499 NSLs. That's about one every ten minutes.

USA Patriot Act (5 of 11)

- Critics of the USA Patriot Act argue that it has a chilling effect on freedom of speech and religion (e.g., mosque attendance has dropped).
- Critics also argue that it undermines the 4th Amendment:
  - It allows gathering Internet metadata, without probable cause.
  - It allow roving surveillance, without describing the locations.
  - It allows, in some cases, warrantless tangible search and seizure.
  - It allows records seizure, without probable cause.
- 2009: Google's CEO Eric Schmidt said:
  pub/ch6/Schmidt.txt

USA Patriot Act (6 of 11)

- Since its enactment:
  - Terrorism charges have been brought against 361 people.
  - Of these, 191 people have been convicted or pled guilty.
  - More than 500 people linked to the World Trade Center and Pentagon attacks have been removed from the US.
  - Terrorist "cells" in the US have been destroyed.

USA Patriot Act (7 of 11)

- Also, since its enactment, innocent people have been monitored, arrested, detained, and abused. For example:
  - In 2004, the FBI did all of this to attorney Brandon Mayfield, from Portland, Oregon.
  - He was jailed for two weeks.
  - The FBI affidavit, to get an arrest warrant, noted that he was Muslim, with an Egyptian-born wife.
  - In 2006, he received a formal apology and $2 million.

USA Patriot Act (8 of 11)

- 2011: US Senator Wyden (OR):
  "...when the American people find out how their government has interpreted the Patriot Act, they will be stunned and they will be angry."
- 2014: Edward Snowden describes how the FBI requested the FISA Court, to order Verizon, to provide the NSA with daily logs of customer cell-phone calls, for three months.
- Metadata was requested, not call content.
- Verizon could not disclose the order.

USA Patriot Act (9 of 11)

- President Obama confirmed Snowden's leak. His administration said it was authorized by the Patriot Act, and that court orders for phone records "... are something that have been in place for a number of years now."
- US Senator Feinstein (CA), and Chair of the Intelligence Committee, confirmed: "As far as I know, this is an exact three-month renewal of what has been the case for the last seven years."

USA Patriot Act (10 of 11)

- US Senator Udall (AZ): "This sort of wide-scale surveillance should concern all of us and is the kind of government overreach I've said Americans would find shocking."
- Former Vice President Al Gore: the blanket order is "obscenely outrageous."
- US Congressman and Patriot Act author, Jim Sensenbrenner (WI): "I do not believe the broadly drafted FISA order is consistent with the requirements of the Patriot Act. Seizing phone records of millions of innocent people is excessive and un-American."

USA Patriot Act (11 of 11)

- 2015: A US Court of Appeals rules that the FBI/NSA/Verizon bulk-records collection program is illegal.
- The Court said it was unreasonable to interpret the Patriot Act as authorizing bulk collection of phone records.
- 2015: The relevant section of the Patriot Act expires, but is replaced by the USA Freedom Act. It requires phone companies to collect and store the records, as before, but requires a warrant for government access.

Database regulation (1 of 5)

- We've seen that US citizens submit data to various government agencies (e.g., Census Bureau and IRS). These agencies manage their own databases.
- Federal law requires Census data to be kept confidential. However, during World War I, it was used to pursue draft resisters. During World War II, it was used to identify Japanese-American citizens for illegal internment.
- The NCIC database is known to contain erroneous data and non-crime data (e.g., about war protesters). It allows illegal searches, sales, and modifications of data.
- The OneDOJ database contains unverified and uncorrectable data.

Database regulation (2 of 5)

- 1965: The Bureau of the Budget forms a committee to study and improve the fragmentation problem. The committee recommends the creation of a National Data Center.
- There was immediate public and congressional outcry, about potential misuses of such a massive centralized database.
- Congress formed the Special Subcommittee on Invasion of Privacy, to study the problem.
- 1972: A committee of the US Department of Health, Education, and Welfare develops the Code of Fair Information Practices:

  `pub/ch6/fip.txt`
- Several European countries produced similar codes.

Database regulation (3 of 5)

- 1974: Congress turns the Code of Fair Information into the Privacy Act of 1974. However:
  - It applies only to government databases.
  - It covers only records *indexed* by a person's identifier.
  - No agency is in charge of enforcement, so an agency can exempt a database.
  - Agencies can share data for "routine use."
- Congress has also passed laws for privately managed databases, which we'll see next.

Database regulation (4 of 5)

- 1970: The Fair Credit Reporting Act regulates the collection, dissemination, and use of consumer information, including consumer credit information. It limits retention of most negative data to seven years.
- 2004: The Fair and Accurate Credit Transactions Reporting Act requires credit bureaus to provide consumers a free copy of their report, annually. It also has provisions to reduce and mitigate identity theft.
- A 2015 FTC study showed that 23% of consumers reported inaccuracies in their credit report.

Database regulation (5 of 5)

- 1999: The Financial Services Modernization Act requires financial institution to disclose their privacy policies to consumers, and provide an opt-out choice for data sharing/selling.

Government data mining (1 of 2)

- The IRS uses algorithms on submitted tax data, to detect unreported income and other irregularities. 60% of audits start this way.
- The WHO and CDC use algorithms on multiple databases, to detect systemic public-health problems.
- The NSA uses algorithms on phone-record metadata, to detect terrorist activity.
  In 2006, this database comprised metadata submitted voluntarily, without a warrant. A US judge ruled the program illegal and unconstitutional. A US Court of Appeals overturned the ruling: the plaintiffs weren't the actual victims.

Government data mining (2 of 2)

- Police departments use algorithms on recent-crime databases, to predict "hotspots" for officer deployment.
- Data mining is used for targeted advertising, showing a potential customer products of predicted personal interest.
- Similarly, it can be used to search one or more databases, for people matching a predicted profile of a criminal or terrorist.
- For example, The US Terrorist Screening Database is a "watch list" of 1.5 million people.

National identification (ID) card (1 of 2)

- In a database, a person's data is identified by some kind of key (e.g., student ID number).
- To avoid confusion, keys must be unique.
- In a national database, containing data for all inhabitants, what can we use for a key?
  - Last name, full name, gender, birthdate, hair color, eye color? They are not one-to-one.
  - Social Security number (SSN)? Not everyone has one. They are not one-to-one.
  - Address, phone number, email address? Not everyone has one. They change.
  - Driver's license number? Not everyone has one. They are managed by states. They change.
  - Biometric data (e.g., fingerprint)? Privacy violation. Complex. Hard to gather.

National ID card (2 of 2)

- What if every inhabitant was assigned a unique number?
- We could stamp it (somehow) on a card, and give it to the person.
- It would be like a universal, one-to-one, SSN, but:
  - Is the card the ID? How do I prove it's my card? Are we back to biometric data?
  - Is the number the ID?
  - Can an invalid number be detected?
  - Can a valid number be guessed?
- What else is recorded on the card? Nothing? Everything? Is it encrypted? How?
- What happens when a card is lost or stolen?

National ID card benefits

- It would be more reliable than current ID.
- It would reduce illegal immigration.
- It would reduce crime.
- It would not violate privacy.

National ID card harms

- It would not guarantee a person's authenticity. A card can be stolen or forged.
- All biometric-ID systems suffer from false-positive and false-negative matches.
- There is no evidence it would reduce crime.
- It would simplify government data mining. Peter Neumann and Laura Weinstein write:

  pub/ch6/Neumann.txt
- Centralized personal data, about law-abiding people, could be inaccurate, due to mistakes or fraud caused by other, non-governmental, people of authority (e.g., teachers or doctors).

The REAL ID Act (1 of 2)

- 2005: George W. Bush signs the law, to make state drivers' licenses a more reliable form of ID.
- Critics say it creates a de facto national ID card.
- It requires states to issue new licenses. Applicants must provide four forms of ID, verified by state employees against federal databases.
- The new licenses must conform to federal requirements: digital photograph, machine-readable, tamper-resistant, etc.
- They are required for many federal activities (e.g., open a bank account or board a commercial airplane).

The REAL ID Act (2 of 2)

- Proponents say it makes for more reliable identification. You can't just go to another state and get a license under another name.
- Opponents say it increases the risk of identity theft. All states must share the machine-readable data. An ACLU lawyer Timothy Sparapani writes:

  pub/ch6/ACLU.txt
- A retailer can record and sell this same information, by scanning a license.

Data dissemination (1 of 2)

- Several US laws regulate how information is shared: some restrict sharing, while others promote it.
- 1974: The Family Educational Rights and Privacy Act (FERPA) requires educational institutions to keep student data private. It also allows students to review and correct their data.
- 1988: The Video Privacy Protection Act requires video providers (e.g., DVD rental stores) to keep customer data private.
- 1996: The Health Insurance Portability and Accountability Act (HIPAA) restricts how organizations in the medical industry can use/share patient data. It also allows patients to review and correct their data.

Data dissemination (2 of 2)

- 1966: The Freedom of Information Act requires the executive branch (only) of the US government to release requested data, or explain why it will not. Exceptions: national-security secrets, trade secrets, confidential commercial/financial data, law-enforcement data, etc.
- Recall our (hypothetical) scenario about the East Dakota State Police giving video, recorded for traffic-law enforcement, to the FBI for terrorist investigation. Is that the "routine use" discussed in the Privacy Act of 1974?
- Our textbook describes the (real-life) E-ZPass toll-collection system, where traffic data is shared, by court order, for criminal (e.g., murder) and civil (e.g., divorce) cases. E-ZPass is *not* a government database, so the "routine use" clause of the Privacy Act does not apply.

Privacy invasion (1 of 2)

- We described privacy as a "zone of inaccessibility." It includes the right to be left alone.
- 2003: The National Do Not Call Registry is a free service, allowing people to register their phone numbers. Telemarketers cannot call phones on the list. Exceptions: politics, charities, and surveys. 50 million phones were registered, before it even started.
- 2010: The Commercial Advertisement Loudness Mitigation Act requires TV commercials to be no louder than regular content.

Privacy invasion (2 of 2)

- 2007: Advanced imaging technology (AIT) scanners are added to TSA security screening, at airports. They reveal "all anatomical features" in a warrantless "virtual strip-search," without probable cause. People accuse the TSA of making child pornography.
- 2010: The Electronic Privacy Information Center (EPIC) sues, arguing the program violates the Administrative Procedure Act, the Privacy Act, the Religious Freedom Restoration Act, the Video Voyeurism Prevention Act, and the Fourth Amendment.
- 2011: EPIC "wins," but only because the TSA didn't follow public-comment requirements, before deploying AIT scanners. The TSA announces that in the new system, images are analyzed by computer. No human sees the nudity.

Chapter 7: Computer and network security (1 of 2)

- In this chapter, we consider threats to the security of computer systems, and the networks that interconnect them.
- First, some definitions of the noun "hacker," from The Jargon File and The Free On-line Dictionary of Computing:
  - 1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary. RFC 1392, the Internet Users' Glossary, usefully amplifies this as: A person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular.

Chapter 7: Computer and network security (2 of 2)

(continued)

- 8. [deprecated] A malicious meddler who tries to discover sensitive information by poking around. Hence password hacker, network hacker. The correct term for this sense is "cracker."

- Of course, the deprecated definition is the popular one, and the one used by our textbook.

Penalties for hacking (1 of 2)

- 1986: The Computer Fraud and Abuse Act (CFAA) criminalizes:
  - transmitting code that damages a computer (e.g., a virus)
  - accessing a remote computer, without authorization, regardless of purpose
  - transmitting classified government data
  - buying, selling, or trading computer passwords
  - computer fraud
  - computer extortion

  The maximum penalty is 20 years in prison and a $250,000 fine.
- We already saw the ECPA. It criminalizes intercepting data transmissions and accessing stored email, without authorization.

Penalties for hacking (2 of 2)

- 1872: The Wire Fraud Act applies to the Internet, too.
- 1934?: The National Stolen Property Act criminalizes transportation of stolen goods (e.g., data).
- 1998: The Identity Theft and Assumption Deterrence Act criminalizes identity theft. Further, it establishes that the person whose identity was stolen is a victim, too.

Case study: Firesheep (1 of 6)

- Since the Internet was developed among trusting parties, communication was expected to be unencrypted (i.e., plaintext).
- Encryption requires additional computation, and can be somewhat inconvenient.
- Typically, adding encryption to a protocol breaks backward compatability, so administrators are reluctant to change.
- Even today, email is very rarely encrypted.
- The Domain Name System (DNS) employs authentication, but not encryption.

Firesheep (2 of 6)

- The WWW uses two primary ports/protocols: HTTP (port 80) and HTTPS (port 443). HTTP is unencrypted. HTTPS is encrypted, via Transport Level Security (TLS), nee Secure Sockets Layer (SSL).
- TLS authentication uses public-key cryptography (asymmetric keys). A digital certificate establishes trust in a public key.
- TLS encryption uses symmetric cryptography. The key is negotiated just after authentication.
- Some websites use a shortcut. They encrypt over HTTPS for user/password authentication, then revert to unencrypted HTTP for the rest of the connection.

Firesheep (3 of 6)

- A file called a *cookie* records connection-related information, and allows the connection to continue without further authentication.
- A cookie is stored on the client (i.e., the browser's computer). It may be sent from the server to the client over HTTPS or HTTP. If HTTP, the cookie may be intercepted, by sniffing the media (e.g., cable or wireless network).

Firesheep (4 of 6)

- Independent of packet-payload encryption (e.g., HTTPS), a wireless network can be unencrypted (aka, *open*) or encrypted.
- There are several wireless-encryption protocols (e.g., WEP and WPA). WEP is weakly encrypted, thus, effectively open. WPA is strongly encrypted.
- Many retailers provide open wireless networks.

Firesheep (5 of 6)

- Firesheep is a Firefox-browser plugin that intercepts someone else's website cookie, sent over an open wireless network, over (unencrypted) HTTP. A hacker can use that cookie to *sidejack* a WWW connection, masquerading as the previously authenticated user.
- Firesheep was developed and released, in 2010, by Eric Butler. His goal was to raise awareness of the vulnerability, and spur website operators, and wireless-network operators, to adopt better encryption practices. Basically, he packaged pre-existing tools, to create an easy-to-use plugin.

Firesheep (6 of 6)

- In the first week, it was downloaded a half million times. Responding to criticism, Butler wrote: "Criminals already know this, and I reject the notion that something like Firesheep turns otherwise innocent people evil."
- Soon after, Facebook and Twitter offered an opt-in all-HTTPS option, to plug the hole.
- Was Butler's release of Firesheep moral?