A Gift of Fire

Fourth edition

Sara Baase

Chapter 1:
Unwrapping the Gift

Slides prepared by Cyndi Chie and Sarah Frye. Fourth edition revisions by Sharon Gray.

What We Will Cover

- The Pace of Change
- Change and Unexpected Developments
- Themes
- Ethics

The Pace of Change

*"In a way not seen since Gutenberg's printing press
that ended the Dark Ages and ignited the Renaissance,
the microchip is an epochal technology with unimaginably
far-reaching economic, social, and political consequences."*

– Michael Rothschild[1]

The Pace of Change

Discussion Question

What devices are now computerized that were not originally? Think back 10, 20, 50 years ago.

Corresponding page number: 4-6

Change and Unexpected Developments

Cell Phones

- Relatively few in 1990s. Approximately five billion worldwide in 2011.
- Used for conversations and messaging, but also for:
  - taking and sharing pictures
  - downloading music and watching videos
  - checking email and playing games
  - banking and managing investments
  - finding maps
- Smartphone apps for many tasks, including:
  - monitoring diabetes
  - locating water in remote areas

Corresponding page number: 7-8

Change and Unexpected Developments

Cell Phones (cont.):

- Location tracking raises privacy concerns.
- Cameras in cell phones affect privacy in public and non-public places.
- Cell phones can interfere with solitude, quiet and concentration.
- Talking on cell phones while driving is dangerous.
- Other unanticipated negative applications: teenagers sexting, terrorists detonating bombs, rioters organizing looting parties.

Corresponding page number: 8-9

Change and Unexpected Developments

Kill switches

- Allow a remote entity to disable applications and delete files.
- Are in operating systems for smartphones, tablets and some computers.
- Used mainly for security, but raise concerns about user autonomy.

Corresponding page number: 9-10

Change and Unexpected Developments

Social Networking:

- First online social networking site was www.classmates.com in 1995.
- Founded in 2003, Myspace had roughly 100 million member profiles by 2006.
- Facebook was started at Harvard as an online version of student directories
- Social networking is popular with hundreds of millions of people because of the ease with which they can share aspects of their lives.

Change and Unexpected Developments

Social Networking (cont.):

- Businesses connect with customers.
- Organizations seek donations.
- Groups organize volunteers.
- Protesters organize demonstrations and revolutions.
- Individuals pool resources through “crowd funding”.

Corresponding page number: 10-11

Change and Unexpected Developments

Social Networking (cont.):

- Stalkers and bullies stalk and bully.
- Jurors tweet about court cases during trials.
- Socialbots simulate humans.

Corresponding page number: 10-11

Change and Unexpected Developments

Telemedicine

- Remote performance of medical exams and procedures, including surgery.

Corresponding page number: 14

Change and Unexpected Developments

Free stuff

- Email programs and email accounts, browsers, filters, firewalls, encryption software, word processors, spreadsheets, software for viewing documents, software to manipulate photos and video, and much more
- Phone services using VOIP such as Skype
- Craigslist classified ad site
- University lectures

Change and Unexpected Developments

Free stuff (cont.)

- Advertising pays for many free sites and services, but not all.
- Wikipedia funded through donations.
- Businesses provide some services for good public relations and as a marketing tool.
- Generosity and public service flourish on the Web. Many people share their expertise just because they want to.

Corresponding page number: 16-17

Change and Unexpected Developments

Free stuff (cont.)

- In order for companies to earn ad revenue to fund multimillion-dollar services, many free sites collect information about our online activities and sell it to advertisers.

Corresponding page number: 17

Change and Unexpected Developments

Artificial intelligence

- A branch of computer science that makes computers perform tasks normally requiring human intelligence.
- Researchers realized that narrow, specialized skills were easier for computers than what a five-year-old does: recognize people, carry on a conversation, respond intelligently to the environment.

Corresponding page number: 17

Change and Unexpected Developments

Artificial intelligence (cont.)

- Many AI applications involve pattern recognition.
- Speech recognition is now a common tool.

Corresponding page number: 18

Change and Unexpected Developments

Artificial intelligence (cont.)

- Turing Test: If the computer convinces the human subject that the computer is human, the computer is said to “pass”.

Corresponding page number: 18

Change and Unexpected Developments

Discussion Questions

How will we react when we can go into a hospital for surgery performed entirely by a machine? Will it be scarier than riding in the first automatic elevators or airplanes?

How will we react when we can have a conversation and not know if we are conversing with a human or a machine?

How will we react when chips implanted in our brains enhance our memory with gigabytes of data and a search engine? Will we still be human?

Corresponding page number: 19

Ethics

What is Ethics:

- Study of what it means to “do the right thing”.
- Assumes people are rational and make free choices.
- Rules to follow in our interactions and our actions that affect others.

Corresponding page number: 26-27

Ethics

A variety of ethical views (cont.):

- Golden rules
  - Treat others as you would want them to treat you.
- Contributing to society
  - Doing one’s work honestly, responsibly, ethically, creatively, and well is virtuous.

Corresponding page number: 32-33

Ethics

A variety of ethical views (cont.):

- No simple answers
  - Human behavior and real human situations are complex. There are often trade-offs to consider.
  - Ethical theories help to identify important principles or guidelines.

Corresponding page number: 35-36

Ethics

A variety of ethical views (cont.):

- Do organizations have ethics?
  - Ultimately, it is individuals who are making decisions and taking actions. We can hold both the individuals and the organization responsible for their acts.

Corresponding page number: 36

A Gift of Fire

Fourth edition

Sara Baase

Chapter 2: Privacy

Slides prepared by Cyndi Chie and Sarah Frye. Fourth edition revisions by Sharon Gray.

Privacy Risks and Principles

Key Aspects of Privacy:

- Freedom from intrusion (being left alone)
- Control of information about oneself
- Freedom from surveillance (from being tracked, followed, watched)

Privacy Risks and Principles

Privacy threats come in several categories:

- Intentional, institutional uses of personal information
- Unauthorized use or release by "insiders"
- Theft of information
- Inadvertent leakage of information
- Our own actions

Corresponding page number: 49

Privacy Risks and Principles

New Technology, New Risks:

- Government and private databases
- Sophisticated tools for surveillance and data analysis
- Vulnerability of data

Corresponding page number: 50-51

Privacy Risks and Principles

New Technology, New Risks – Examples:

Smartphones

- Location apps
- Data sometimes stored and sent without user’s knowledge

Corresponding page number: 53-54

Privacy Risks and Principles

New Technology, New Risks – Summary of Risks:

- Anything we do in cyberspace is recorded.
- Huge amounts of data are stored.
- People are not aware of collection of data.
- Software is complex.
- Leaks happen.

Corresponding page number: 55

Privacy Risks and Principles

Fair information principles

1. Inform people when you collect information.
2. Collect only the data needed.
3. Offer a way for people to opt out.
4. Keep data only as long as needed.
5. Maintain accuracy of data.
6. Protect security of data.
7. Develop policies for responding to law enforcement requests for data.

Corresponding page number: 60

The Fourth Amendment

The right of the people to be secure in their person, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

—4th Amendment, U.S. Constitution

The Fourth Amendment

- Sets limits on government’s rights to search our homes and businesses and seize documents and other personal effects. Requires government provide probable cause.
- Two key problems arise from new technologies:
  - Much of our personal information is no longer safe in our homes; it resides in huge databases outside our control.
  - New technologies allow the government to search our homes without entering them and search our persons from a distance without our knowledge.

Corresponding page number: 61-62

New Technologies

- Make possible “noninvasive but deeply revealing” searches
  - particle sniffers, imaging systems, location trackers
- What restrictions should we place on their use? When should we permit government agencies to use them without a search warrant?

Supreme Court Decisions and Expectation of Privacy

- *Katz v United States* (1967)
  - Supreme Court reversed its position and ruled that the Fourth Amendment *does* apply to conversations.
  - Court said that the Fourth Amendment protects people, not places. To intrude in a place where reasonable person has a reasonable expectation of privacy requires a court order.

Corresponding page number: 64

Supreme Court Decisions and Expectation of Privacy

- *Kyllo v United States* (2001)
  - Supreme Court ruled that police could not use thermal-imaging devices to search a home from the outside without a search warrant.
  - Court stated that where “government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a ‘search.’”

Corresponding page number: 64

Search and Seizure of Computers and Phones

- How should we interpret “plain view” for search of computer or smartphone files?

Corresponding page number: 66-68

Video Surveillance and Face Recognition

- Security cameras
  - Increased security
  - Decreased privacy

Corresponding page number: 68-70

Marketing and Personalization

- Data mining
- Targeted ads

Corresponding page number: 70-74

Social Networks

- What *we* do
  - Post opinions, gossip, pictures, “away from home” status
- What *they* do
  - New services with unexpected privacy settings

Corresponding page number: 75-77

Our Social and Personal Activity

Discussion Questions

- *Is there information that you have posted to the Web that you later removed? Why did you remove it? Were there consequences to posting the information?*
- *Have you seen information that others have posted about themselves that you would not reveal about yourself?*

Corresponding page number: 75-77

A Gift of Fire

Fourth edition

Sara Baase

Chapter 3: Freedom of Speech

Slides prepared by Cyndi Chie and Sarah Frye. Fourth edition revisions by Sharon Gray.

Communication Paradigms

Regulating communications media

- First Amendment protection and government regulation
  - Print media (newspapers, magazines, books)
  - Broadcast (television, radio)
  - Common carries (telephones, postal system)

Corresponding page number: 134-136

Communication Paradigms

Telecommunication Act of 1996

- Changed regulatory structure and removed artificial legal divisions of service areas and restrictions on services that telephone companies can provide.
- No provider or user of interactive computer services shall be treated as a publisher of any information provided by another information-content provider.

Corresponding page number: 137

Communication Paradigms

Free-speech Principles

- Written for offensive and/or controversial speech and ideas
- Covers spoken and written words, pictures, art, and other forms of expression of ideas and opinions
- Restriction on the power of government, not individuals or private businesses

Corresponding page number: 137-138

Controlling Speech

Offensive speech: What is it? What is illegal?

- Answers depend on who you are.
- Most efforts to censor the Internet focus on pornographic and other sexually explicit material

Controlling Speech

What was already illegal?

- Obscenity
  - Depicts a sexual act against state law
  - Depicts these acts in a patently offensive manner that appeals to prurient interest as judged by a reasonable person using community standards
  - Lacks literary, artistic, social, political or scientific value

Corresponding page number: 140

Controlling Speech

Freedom of speech guidelines

- Distinguish speech from action. Advocating illegal acts is (usually) legal.
- Laws must not chill expression of legal speech.
- Do not reduce adults to reading only what is fit for children.
- Solve speech problems by least restrictive means.

Corresponding page number: 142

Controlling Speech

Discussion Question

- *Why is ‘least restrictive means’ important?*
- *Do you consider the Internet an appropriate tool for young children? Why or why not?*

Corresponding page number: 141-145

Posting, Selling, and Leaking Sensitive Material

“Free speech is enhanced by civility.”

-Tim O’Reilly

Corresponding page number: 153

Posting, Selling, and Leaking Sensitive Material

- Policies of large companies
- A Web site with risks

Corresponding page number: 154-155

Posting, Selling, and Leaking Sensitive Material

- Leaks
  - Type of material
  - Value to society
  - Risks to society and individuals

Corresponding page number: 155-156

Posting, Selling, and Leaking Sensitive Material

- Leaks (cont.)
  - Examples
    - WikiLeaks
    - Climategate

Corresponding page number: 156-157

Posting, Selling, and Leaking Sensitive Material

Discussion Question

- *Does the value of informing the public of controversial and sensitive information outweigh the dangers and risks?*

Corresponding page number: 155-156

Anonymity

- Positive uses of anonymity
  - Protect political speech
  - Protect against retaliation and embarrassment
- Anonymizing services
  - used by individuals, businesses, law enforcement agencies, and government intelligence services

Corresponding page number: 159-161

Anonymity

- Negative uses of anonymity
  - protects criminal and antisocial activities
  - aids fraud, harassment, extortion, distribution of child pornography, theft, and copyright infringement
  - masks illegal surveillance by government agencies

Corresponding page number: 161-162

A Gift of Fire

Fourth edition

Sara Baase

Chapter 5:
Crime

Slides prepared by Cyndi Chie and Sarah Frye. Fourth edition revisions by Sharon Gray.

What We Will Cover

- Hacking
- Identity Theft and Credit Card Fraud
- Whose Laws Rule the Web

Corresponding page number: 229

Hacking

- Intentional, unauthorized access to computer systems
- The term has changed over time
- Phase 1: The joy of programming
  - Early 1960s to 1970s
  - It was a positive term
  - A "hacker" was a creative programmer who wrote elegant or clever code
  - A "hack" was an especially clever piece of code

Corresponding page number: 230-231

Hacking

Phase 2: 1970s to mid 1990s

- Hacking took on negative connotations
- Breaking into computers for which the hacker does not have authorized access
- Still primarily individuals
- Includes the spreading of computer worms and viruses and ‘phone phreaking’
- Companies began using hackers to analyze and improve security

Corresponding page number: 231-232

Hacking

Phase 3: The growth of the Web and mobile devices

- Beginning in mid 1990s
- The growth of the Web changed hacking; viruses and worms could be spread rapidly
- Political hacking (Hacktivism) surfaced
- Denial-of-service (DoS) attacks used to shut down Web sites
- Large scale theft of personal and financial information

Corresponding page number: 232-235

Hacking

Is “harmless hacking” harmless?

- Responding to nonmalicious or prank hacking uses resources.
- Hackers could accidentally do significant damage.
- Almost all hacking is a form of trespass.

Hacking

Hacktivism, or Political Hacking

- Use of hacking to promote a political cause
- Disagreement about whether it is a form of civil disobedience and how (whether) it should be punished
- Some use the appearance of hacktivism to hide other criminal activities
- How do you determine whether something is hacktivism or simple vandalism?

Corresponding page number: 236-237

Hacking

Hackers as Security Researchers

- “White hat hackers” use their skills to demonstrate system vulnerabilities and improve security

Corresponding page number: 237-239

Hacking

Hacking as Foreign Policy

- Hacking by governments has increased
- Pentagon has announced it would consider and treat some cyber attacks as acts of war, and the U.S. might respond with military force.
- How can we make critical systems safer from attacks?

Corresponding page number: 239-240

Hacking

Stuxnet

- An extremely sophisticated worm
- Targets a particular type of control system
- Beginning in 2008, damaged equipment in a uranium enrichment plant in Iran

Corresponding page number: 240

Hacking

Security

- Hacking is a problem, but so is poor security.
- Variety of factors contribute to security weaknesses:
  - History of the Internet and the Web
  - Inherent complexity of computer systems
  - Speed at which new applications develop
  - Economic and business factors
  - Human nature

Corresponding page number: 241-244

Hacking

Security

- Internet started with open access as a means of sharing information for research.
- Attitudes about security were slow to catch up with the risks.
- Firewalls are used to monitor and filter out communication from untrusted sites or that fit a profile of suspicious activity.
- Security is often playing catch-up to hackers as new vulnerabilities are discovered and exploited.

Corresponding page number: 241-244

Hacking

Responsibility for Security

- Developers have a responsibility to develop with security as a goal.
- Businesses have a responsibility to use security tools and monitor their systems to prevent attacks from succeeding.
- Home users have a responsibility to ask questions and educate themselves on the tools to maintain security (personal firewalls, anti-virus and anti-spyware).

Corresponding page number: 244-245

Hacking

Discussion Questions

- *Is hacking that does no direct damage a victimless crime?*
- *Do you think hiring former hackers to enhance security is a good idea or a bad idea? Why?*

Corresponding page number: 230-245

Hacking

The Law: Catching and Punishing Hackers

- 1984 Congress passed the Computer Fraud and Abuse Act (CFAA)
  - Covers government computers, financial and medical systems, and activities that involve computers in more than one state, including computers connected to the Internet
  - Under CFAA, it is illegal to access a computer without authorization
  - The USA PATRIOT Act expanded the definition of loss to include the cost of responding to an attack, assessing damage and restoring systems

Corresponding page number: 245

Hacking

The Law: Catching and Punishing Hackers

- Catching hackers
  - Law enforcement agents read hacker newsletters and participate in chat rooms undercover
  - They can often track a handle by looking through newsgroup or other archives
  - Security professionals set up ‘honey pots’ which are Web sites that attract hackers, to record and study
  - Computer forensics specialists can retrieve evidence from computers, even if the user has deleted files and erased the disks
  - Investigators trace viruses and hacking attacks by using ISP records and router logs

Hacking

The Law: Catching and Punishing Hackers

- Penalties for young hackers
  - Many young hackers have matured and gone on to productive and responsible careers
  - Temptation to over or under punish
  - Sentencing depends on intent and damage done
  - Most young hackers receive probation, community service, and/or fines
  - Not until 2000 did a young hacker receive time in juvenile detention

Corresponding page number: 247-248

Hacking

The Law: Catching and Punishing Hackers

- Criminalize virus writing and hacker tools?

Corresponding page number: 248-249

Hacking

The Law: Catching and Punishing Hackers

- Expansion of the Computer Fraud and Abuse Act
  - The CFAA predates social networks, smartphones, and sophisticated invisible information gathering.
  - Some prosecutors use the CFAA to bring charges against people or businesses that do unauthorized data collection.
  - Is violating terms of agreement a form of hacking?

Corresponding page number: 248-249

Identity Theft and Credit Card Fraud

Stealing Identities

- Identity Theft –various crimes in which criminals use the identity of an unknowing, innocent person
  - Use credit/debit card numbers, personal information, and social security numbers
  - 18-29 year-olds are the most common victims because they use the Web most and are unaware of risks
  - E-commerce has made it easier to steal and use card numbers without having the physical card

Corresponding page number: 250-253

Identity Theft and Credit Card Fraud

Stealing Identities

- Techniques used to steal personal and financial information
  - Requests for personal and financial information disguised as legitimate business communication
    - Phishing – e-mail
    - Smishing – text messaging
    - Vishing – voice phishing
  - Pharming – false Web sites that fish for personal and financial information by planting false URLs in Domain Name Servers
  - Online resumés and job hunting sites may reveal SSNs, work history, birth dates and other information that can be used in identity theft

Corresponding page number: 252-253

A Gift of Fire

Fourth edition

Sara Baase

Chapter 6: Work

Slides prepared by Cyndi Chie and Sarah Frye. Fourth edition revisions by Sharon Gray.

What We Will Cover

- Changes, Fears, and Questions
- Impacts on Employment
- Employee Communications and Monitoring

Corresponding page number: 275

Changes, Fears, and Questions

- The introduction of computers in the workplace generated many fears
  - Mass unemployment due to increased efficiency
  - The need for increased skill and training widens the earning gap
- New trends still generating fears
  - Offshoring of jobs will lead to mass unemployment
  - Employers use of technology to monitor their employees

Corresponding page number: 276

Impacts on Employment

Job creation and destruction

- A successful technology eliminates or reduces some jobs but creates others
  - Reduced the need for telephone operators, meter readers, mid-level managers
- New industries arise
  - Internet
  - Cellular communications
- Lower prices increase demand and create jobs
  - Music industry changed from serving the wealthy to serving the masses, employing more than just musicians

Corresponding page number: 277-279

Impacts on Employment

Changing Skills and Skill Levels

- New products and services based on computer technology create jobs in design, marketing, manufacture, sales, customer service, repair, and maintenance.
- The new jobs created from computers are different from the jobs eliminated.
- New jobs such as computer engineer and system analyst jobs require a college degree, where jobs such as bank tellers, customer service representatives and clerks do not.
- Companies are more willing to hire people without specific skills when they can train new people quickly and use automated support systems.

Corresponding page number: 282-284

Impacts on Employment

Discussion Questions

- *What jobs have been eliminated due to technology?*
- *What jobs that were once considered high-skill jobs are now low-skill due to technology?*
- *What new jobs have been created because of technology?*
- *Do automated systems mean fewer jobs for high-skilled workers?*
- *Will human intelligence in employment be "devalued"?*

Corresponding page number: 277-284

Impacts on Employment

Telecommuting

- Working at home using a computer electronically linked to one's place of employment
- Mobile office using a laptop, working out of your car or at customer locations
- Fulltime and part-time telecommuting

Corresponding page number: 284-285

Impacts on Employment

Telecommuting

- Benefits
  - Reduces overhead for employers
  - Reduces need for large offices
  - Employees are more productive, satisfied, and loyal
  - Reduces traffic congestion, pollution, gasoline use, and stress
  - Reduces expenses for commuting and money spent on work clothes
  - Allows work to continue after blizzards, hurricanes, etc.

Corresponding page number: 285-286

Impacts on Employment

Telecommuting

- Problems
  - Employers see resentment from those who have to work at the office
  - For some telecommuting employees, corporation loyalty weakens
  - Odd work hours
  - Cost for office space has shifted to the employee
  - Security risks when work and personal activities reside on the same computer

Corresponding page number: 286-287

Impacts on Employment

Discussion Questions

- *Would you want to telecommute? Why or why not?*
- *How has technology made entrepreneurship easier? Harder?*

Corresponding page number: 285-287

Impacts on Employment

Personal social media

- Basing disciplinary action on personal, nonwork social media is more controversial because it extends employer control beyond the workplace.
- Content in social media is often widely distributed; thus impact is stronger than that of a private conversation.
- Employer restrictions on nonwork social media do not violate employee’s freedom of speech (unless, in some cases, when the employer is the government).

Corresponding page number: 302-303

Impacts on Employment

Discussion Questions

- *It is reasonable for employers to fire employees for content of their blogs, tweets, or posts on social networks?*
- *Are there good reasons for employers to be concerned about what their employees post in such places?*

Corresponding page number: 302-303

A Gift of Fire

Fourth edition

Sara Baase

Chapter 9:
Professional Ethics and Responsibilities

Slides prepared by Cyndi Chie and Sarah Frye. Fourth edition revisions by Sharon Gray.

What We Will Cover

- What is Professional Ethics?
- Ethical Guidelines for Computer Professionals
- Scenarios

Corresponding page number: 403

What is "Professional Ethics"?

- Professional ethics includes relationships with and responsibilities toward customers, clients, coworkers, employees, employers, others who use one's products and services, and others whom they affect
- A professional has a responsibility to act ethically. Many professions have a code of ethics that professionals are expected to abide by
  - Medical doctors
  - Lawyers and judges
  - Accountants

Corresponding page number: 404-405

What is "Professional Ethics"?

- There are special aspects to making ethical decisions in a professional context
- Honesty is one of the most fundamental ethical values; however, many ethical problems are more subtle than the choice of being honest or dishonest
- Some ethical issues are controversial

Corresponding page number: 404-405

Ethical Guidelines for Computer Professionals

Special Aspects of Professional Ethics

- A professional is an expert in a field
  - Customers rely on the knowledge, expertise, and honesty of the professional
- The work of many professionals profoundly affect large numbers of people, some indirectly
- Professionals must maintain up to date skills and knowledge

Corresponding page number: 405-406

Ethical Guidelines for Computer Professionals

Professional Codes of Ethics

- Provide a general statement of ethical values
- Remind people in the profession that ethical behavior is an essential part of their job
- Provide guidance for new or young members

Corresponding page number: 406-407

Ethical Guidelines for Computer Professionals

Guidelines and Professional Responsibilities

- Understand what success means
- Include users (such as medical staff, technicians, pilots, office workers) in the design and testing stages to provide safe and useful systems
- Do a thorough, careful job when planning and scheduling a project and when writing bids or contracts
- Design for real users

Corresponding page number: 407-410

Ethical Guidelines for Computer Professionals

Guidelines and Professional Responsibilities (cont.)

- Don’t assume existing software is safe or correct; review and test it
- Be open and honest about capabilities, safety, and limitations of software
- Require a convincing case for safety
- Pay attention to defaults
- Develop communication skills

Corresponding page number: 407-410