**CHAPTER 1:**

* 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
  + 1940s: First computer was built.
  + 1956: First hard-drive disk weighed a ton and stored five megabytes.
  + 1991: Space shuttle had a one-megahertz computer. Ten years later, some automobiles had 100-megahertz computers. Speeds of several gigahertz are now common.
* Change and Unexpected Developments: “It is precisely this unique human capacity to transcend the present, to live one’s life by purposes stretching into the future – to live not at the mercy of the world, but as a builder and designer of that world – that is the distinction between human and animal behavior, or between the human being and the machine.” – Betty Friedan
  + 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
    - 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.
  + 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.
  + Social Networking:
    - First online social networking site was [www.classmates.com](http://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.
    - Businesses connect with customers.
    - Organizations seek donations.
    - Groups organize volunteers.
    - Protesters organize demonstrations and revolutions.
    - Individuals pool resources through “crowd funding”.
    - Stalkers and bullies stalk and bully.
    - Jurors tweet about court cases during trials.
    - Socialbots simulate humans.
  + Communication and the Web:
    - In the 1980s, email messages were short and contained only text.
    - People worldwide still use email, but texting, tweeting, and other social media are now preferred.
    - Blogs (“Web log”) began as outlets for amateurs wanting to express ideas, but they have become significant source of news and entertainment.
    - Inexpensive video cameras and video-manipulation tools have resulted in a burst of amateur videos.
    - Many videos on the Web can infringe copyrights owned by entertainment companies.
  + Telemedicine: Remote performance of medical exams and procedures, including surgery.
  + Collaboration:
    - Wikipedia: The online, collaborative encyclopedia written by volunteers.
    - Informal communities of programmers create and maintain free software.
    - Watch-dogs on the Web: Informal, decentralized groups of people that help investigate crimes.
  + E-commerce:
    - Amazon.com started in 1994 selling books on the Web. It has grown to be one of the most popular, reliable, and user-friendly commercial sites.
    - eBay.com facilitates online auctions.
    - Traditional brick-and-mortar business have established Web sites.
    - Online sales in the United States now total hundreds of billions of dollars a year.
    - Sellers can sell directly to buyers, resulting in a peer-to-peer economy.
    - Trust Concerns:
      * People were reluctant to provide credit card information to make online purchases, so PayPal.com grew out of need for trusted intermediary to handle payments.
      * Encryption and secure servers made payments safer.
      * The Better Business Bureau established a Web site to help consumers see if others have complained about a business.
      * Auction sites implemented rating systems.
  + 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.
    - Advertising pays for many free sites and services, but not all.
    - Wikipedia funded through donations.
    - Business 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.
    - 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.
  + Artificial Intelligence:
    - A branch of computer science that makes computers perform tasks normally requiring human intelligence.
    - Researches 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.
    - Many AI applications involve pattern recognition.
    - Speech recognition is now a common tool.
    - Turing Test: If the computer convinces the human subject that the computer is human, the computer is said to “pass”.
  + Robots:
    - Mechanical devices that perform physical tasks traditionally done by humans.
    - Can operate in environments that are hazardous for people.
  + Smart Sensors, Motion, and Control:
    - Motion sensing devices are used to give robots the ability to walk, trigger airbags in a crash, and protect laptops when dropped.
    - Sensors can detect leaks, acceleration, position, temperature, and moisture.
  + Tools for Disabled People:
    - Assistive technology devices help restore productivity and independence to people with disabilities.
    - Researchers are experimenting with chips that convert brain signals to controls for leg and arm muscles.
* Themes of Technology Challenges:
  + Old Problems in a New Context: crime, pornography, violent fiction, etc.
  + Adapting to New Technology: Thinking in a new way.
  + Varied Sources of Solutions to Problems: Natural part of change and life.
  + Global Reach of Net: Ease of communication with distant countries.
  + Trade-offs and Controversy: Increasing security means reducing convenience.
  + Perfection is a direction, not an option.
  + There is a difference between personal choices, business policies, and law.
* 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.
  + A Variety of Ethical Views: Deontological theories, Utilitarianism, & Natural Rights.
    - Negative Rights (Liberties): The right to act without interference.
    - Positive Rights (Claim-rights): An obligation of some people to provide certain things for others.
    - 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.
    - Social Contracts and a Theory of Political Justice: People willingly submit to a common law in order to live in a civil society.
    - 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.
    - 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.
  + Some Important Distinctions:
    - Right, wrong, and okay.
    - Distinguishing wrong and harm.
    - Separating goals from constraints.
    - Personal preference and ethics.
    - Law and ethics.

**CHAPTER 2:**

* 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 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
  + New Technology, New Risks:
    - Government and private databases
    - Sophisticated tools for surveillance and data analysis
    - Vulnerability of data
    - Examples:
      * Search Query Data:
        + Search engines collect many terabytes of data daily.
        + Data is analyzed to target advertising and develop new services.
        + Who gets to see this data? Why should we care?
      * Smartphones:
        + Location apps
        + Data sometimes stored and sent without user’s knowledge
    - 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.
      * A collection of small items can provide a detailed picture.
      * Re-identification has become much easier due to the quantity of information and power of data search and analysis tools.
      * If information is on a public Web site, it is available to everyone.
      * Information on the Internet seems to last forever.
      * Data collected for one purpose will find other uses.
      * Government can request sensitive personal data held by businesses or organizations.
      * We cannot directly protect information about ourselves. We depend upon businesses and organizations to protect it.
  + Terminology:
    - Personal Information: Any information relating to an individual person.
    - Informed Consent: Users being aware of what information is collected and how it is used.
    - Invisible Information Gathering: Collection of personal information about a user without the user’s knowledge.
    - Cookies: Files a Web site stores on a visitor’s computer.
    - Secondary Use: Use of personal information for a purpose other than the purpose for which it was provided.
    - Data Mining: Searching and analyzing masses of data to find patterns and develop new information or knowledge.
    - Computer Matching: Combining and comparing information from different databases (using social security number, for example) to match records.
    - Computer Profiling: Analyzing data to determine characteristics of people most likely to engage in a certain behavior.
  + Two common forms for providing informed consent are opt out and opt in:
    - Opt Out: Person must request (usually by checking a box) that an organization *not* use information.
    - Opt In: The collector of the information may use information only if person explicitly permits use (usually by checking a box).
  + 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.
* 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.”
  + 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.
  + 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:
  + Olmstead vs. United States (1928):
    - Supreme Court allowed the use of wiretaps on telephone lines without a court order.
    - Interpreted the Fourth Amendment to apply only the physical intrusion and only to the search or seizure of material things, not conversations.
  + Katz vs. 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.
  + Kyllo vs. 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.’”
* Search and Seizure of Computers and Phones: How should we interpret “plain view” for search of computer or smartphone files?
* Video Surveillance and Face Recognition:
  + Security cameras – increased security and decreased privacy
* Marketing and Personalization: Data mining & targeted ads
  + Informed consent
  + “Do Not Track” button in browsers
  + Paying for consumer information
* Social Networks
  + What *We* Do: Post opinions, gossip, pictures, “away from home” status.
  + What *They* Do: New services with unexpected privacy settings.
* Life in the Clouds: Security of online data & convenience
* Location Tracking:
  + Global Positioning Systems (GPS): Computer or communication services that know exactly where a person is at a particular time.
  + Cell phones and other devices are used for location tracking.
  + Pros and cons.
  + Tools for Parents: GPS tracking via cell phones or RFID
* A Right to Be Forgotten: The right to have material removed.
  + Negative Right: A Liberty.
  + Positive Right: A claim right.
* Government Systems:
  + Databases:
    - Government Accountability Office (GAO): Monitors government’s privacy policies.
    - Burden of proof and “fishing expeditions”.
    - Data mining and computer matching to fight terrorism.
  + Public Records – Access vs. Privacy:
    - Public Records: Records available to general public (bankruptcy, property, and arrest records, salaries of government employees, etc.)
    - Identity theft can arise when public records are accessed.
    - How should we control access to sensitive public records?
* National ID Systems:
  + Social Security Numbers: Too widely used; easy to falsify.
  + Various new proposals would require citizenship, employment, health, tax, financial, or other data, as well as biometric information. In many proposals, the cards would also access a variety of databases for additional information.
  + A New National ID System – Pros:
    - Would require the card.
    - Harder to forge.
    - Have to carry only one card.
  + A New National ID System – Cons:
    - Threat to freedom and privacy.
    - Increased potential for abuse.
* Protecting Privacy:
  + Technology and Markets:
    - Privacy enhancing-technologies for consumers.
    - Encryption – public key cryptography
    - Business tools and policies for protecting data
* Encryption Policy: Government ban on export of strong encryption software in the 1990s (removed in 2000).
* Rights and Law:
  + Warren and Brandeis: The inviolate personality.
  + Judith Jarvis Thomson: Is there a right to privacy?
  + Transactions
  + Ownership of personal data
  + A Basic Legal Framework: Enforcement of agreements and contracts.
  + Regulation
  + Contrasting Viewpoints:
    - Free Market View:
      * Freedom of consumers to make voluntary agreements.
      * Diversity of individual tastes and values.
      * Response of the market to consumer preferences
      * Usefulness of contracts.
      * Flaws of regulatory solutions.
    - Consumer Protection View:
      * Uses of personal information.
      * Costly and disruptive results of errors in databases.
      * Ease with which personal information leaks out.
      * Consumers need protection from their own lack of knowledge, judgement, or interest.
* Privacy Regulations in the European Union:
  + EU’s rules are more strict than U.S. regulations
  + EU Data Privacy Directive:
    - Prohibits transfer of personal information to countries outside the EU that do not have an adequate system of privacy protection.
    - “Safe Harbor” plan.
    - Abuses still occur.
    - Puts requirements on businesses outside the EU.
* Communications:
  + Wiretapping and Email Protection:
    - Telephone:
      * 1934 Communications Act: Prohibits interception of messages.
      * 1968 Omnibus Crime Control and Safe Streets Act: Allowed wiretapping and electronic surveillance by law-enforcement (with court order).
    - Email and Other New Communications:
      * Electronics Communications Privacy Act of 1986 (ECPA): Extended the 1968 wiretapping laws to include electronic communications, restricts government access to email.
    - The Communications Assistance for Law Enforcement Act (CALEA):
      * Passed in 1994
      * Requires telecommunications equipment be designed to ensure that the government can intercept telephone calls (with a court order or other authorization).
      * Rules and requirements written by Federal Communications Commission (FCC).
* The NSA and Secret Intelligence Gathering:
  + The National Security Agency (NSA):
    - Foreign Intelligence Surveillance Act (FISA) established oversight rules for the NSA.
  + Secret access to communications records.

**CHAPTER 3:**

* Communication Paradigms:
  + Regulating Communications Media:
    - First Amendment Protection and Government Regulation:
      * Print media (newspapers, magazines, books)
      * Broadcast (television, radio)
      * Common carries (telephones, postal system)
    - 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.
  + Communications Decency Act of 1996:
    - First major Internet censorship law
    - Main parts ruled unconstitutional
  + 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.
    - Supreme Court principles and guidelines:
      * Advocating illegal acts is (usually) legal.
      * Anonymous speech is protected.
      * Some restrictions are allowed on advertising.
      * Libel and direct or specific threats are not protected.
      * Inciting violence is illegal.
* 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.
  + 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.
  + Straining old legal standards…
    - The definition of “community”
    - The definition of “distribution”
  + 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.
  + Internet Censorship Laws & Alternatives:
    - Communications Decency Act of 1996 (CDA):
      * Attempted to avoid conflict with First Amendment by focusing on children.
      * Made it a crime to make available to anyone under 18 any obscene or indecent communication.
    - Found to be Unconstitutional:
      * The worst material threatening children was already illegal.
      * It was too vague and broad.
      * It did not use the least restrictive means of accomplishing the goal of protecting children.
    - Child Online Protection Act of 1998 (COPA):
      * More limited than CDA.
      * Federal crime for commercial Web sites to make available to minors material “harmful to minors” as judged by community standards.
    - Found to be Unconstitutional:
      * It was too broad.
      * It would restrict the entire country to the standards of the most conservative community.
      * It would have a chilling effect.
    - Children’s Internet Protection Act of 2000 (CIPA): Requires schools and libraries that participate in certain federal programs to install filtering software.
    - Upheld in Court:
      * Does not violate First Amendment since it does not require the use of filters, impose jail or fines.
      * It sets a condition for receipt of certain federal funds.
    - Video Games:
      * A California law banned sale or rental of violent video games to minors.
      * In 2011, the Supreme Court of California ruled it violated the First Amendment.
    - Alternatives to Censorship:
      * Filters:
        + Blocks sites with specific words, phrases or images.
        + Parental control for sex and violence.
        + Updated frequently but may still screen out too much or too little.
        + Not possible to eliminate all errors.
        + What should be blocked?
      * Policies:
        + Commercial services, online communities, and social networking sites develop policies to protect members.
        + Video game industry developed rating system that provides an indication for parents about the amount of sex, profanity, and violence in a game.
  + Child Pornography:
    - Includes pictures or videos of actual minors (children under 18) engaged in sexually explicit conduct.
    - Production is illegal primarily because of abuse of the actual children, not because of the impact of the content on a viewer.
    - Congress extended the law against child pornography to include “virtual” child pornography.
    - The Supreme Court ruled the law violated the First Amendment.
    - The Court accepted a later law providing harsh penalties for certain categories of computer-generated and cartoon-type images.
  + Sexting:
    - Sending sexually suggestive or explicit text or photos, usually by cellphone or social media.
    - Can meet the definition of child pornography if subject is under 18.
  + Spam:
    - What’s the problem?
      * Loosely described as unsolicited bulk email.
      * Mostly commercial advertisement.
      * Angers people because of content and the way it’s sent.
    - Free Speech Issues:
      * Spam imposes a cost on recipients.
      * Spam filters do not violate free speech (free speech does not require anyone to listen).
    - Anti-Spam Laws:
      * Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act).
      * Targets commercial spam.
      * Criticized for not banning all spam, legitimized commercial spam.
* Posting, Selling, and Leaking Sensitive Material:
  + Policies of large companies.
  + A Web site with risks.
  + Leaks:
    - Type of material
    - Value to society
    - Risks to society and individuals
    - Examples: WikiLeaks and Climategate
    - Potentially dangerous leaks.
    - Releasing a huge mass of documents.
    - Responsibilities of operators of Web sites for leaks.
* Anonymity: *Common Sense* and Federalist Papers
  + Positive Uses of Anonymity:
    - Protect political speech.
    - Protect against retaliation and embarrassment.
  + 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.
  + Anonymizing Services: Used by individuals, businesses, law enforcement agencies, and government intelligence services.
  + Is it Protected?: Many legal issues about anonymity are similar to those discussed in Chapter 2.
* The Global Net – Censorship and Political Freedom:
  + Tools for communication, tools for oppression…
    - Authoritarian governments have impeded flow of information and opinion throughout history.
    - The vibrant communication of the Internet threatens governments in countries that lack political and cultural freedom.
    - Attempts to limit the flow of information on the Internet similar to earlier attempts to place limits on other communications media.
    - Some countries own the Internet backbone within their countries and block specific sites and content at the border.
    - Some countries ban all or certain types of access to the Internet.
    - Avoiding Censorship: The global nature of the Net allows restrictions (or barriers) in one country to be circumvented by using networks in other, less restrictive countries.
    - Creating Censorship: The global nature of the Net makes it easier for one nation to impose restrictive standards on others.
  + “The office of communications is ordered to find ways to ensure that the use of the Internet becomes impossible. The Ministry for the Promotion of Virtue and Prevention of Vice is obliged to monitor the order and punish violators.” – Excerpt from Taliban edict banning Internet use in Afghanistan (2001).
  + Aiding foreign censors and repressive regimes...
    - Yahoo and French Censorship: Yahoo, eBay and others make decisions to comply with foreign laws for business reasons.
    - Skype and Chinese Control: Chinese government requires modified version of Skype.
    - Companies who do business in countries that control Internet access must comply with the local laws.
    - Google argued that some access is better than no access.
  + Selling Surveillance Tools:
    - Repressive governments intercept citizens’ communications and filter Internet content.
    - Companies in Western democracies sell them the sophisticated tools to do so.
  + Shutting Down Communications in Free Countries:
    - Public safety.
    - In the U.S., the Supreme Court would probably declare unconstitutional a law that authorized a government agency to order a private communications service to shut down.
* Net Neutrality Regulations or the Market?:
  + Net Neutrality: Refers to a variety of proposals for restrictions on how telephone and cable companies interact with their broadband customers and set fees for services.
    - Argue for equal treatment of all customers.
  + Market: Flexibility and market incentives will benefit customers.