Chapter 1 Ethics

- Kill switches: The ability to remove applications and files without user consent
- The Internet of Things: everything that is connected to the internet (example: television, webcams, refrigerators, etc)
- Free things are not actually free. They are supported by either ads or donations.
- Artificial intelligence: A branch of computer science that makes computers perform tasks normally requiring human intelligence
- Global reach of Net: ease of communication with distant countries
- Ethical rules:
  - Achieve good results for people in general
  - Ethical theories attempt to achieve the same goal: to enhance human dignity, peace, happiness, and well-being
  - Ethical rules are good and work for people (do what is right. Don't steal)
- Deontological theories
  - View acts as good or bad based on the intrinsic aspect of the action
  - An act is ethical if it complies with ethical rules and you chose it for that reason
  - Immanuel Kant
    - The principle of universality: we should follow rules of behavior that we can universally apply to everyone
    - Follow rationality is ethical: "Respect the reason in you"
    - Principle about interacting with other people: One must never treat people as merely means to ends, but rather as ends in themselves.
- Utilitarianism (Consequentialist)
  - Consider consequences, aim to increase happiness, or net aggregate (utility)
  - Utility: what satisfies a person's needs and values
  - Aggregate utility: consider all affected people
  - Act: Consider utility of each act
  - Rule: Consider utility of general ethic rules instead, not individual act
- Natural rights: try to let people make their own decisions
  - Life: everyone is entitled to live
  - Liberty: everyone is entitled to do anything they want to so long as it doesn't conflict with the first right
  - Property/Estate: everyone is entitled to own all they create or gain through gift or trade so long as it doesn't conflict with the first two rights
- Negative rights (liberties)
  - The rights to act without interference (speech, live, religion, etc.)
- Positive rights (claim-rights)
  - An obligation of some people to provide certain things for others, such as work, food, medical care etc.
- Golden rule
  - Treat others as you want them to treat you

Chapter 2 Privacy

- Three key aspects of privacy
  - Freedom from intrusion: being left alone

- o Control of information about oneself
- o Freedom from surveillance
- Personal information: any information relating to an individual person
- Informed consent: users being aware of what info is collected and how it is used
- Invisible information gathering: collection of personal information about someone without the persons' 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 info or knowledge
- (Computer) Matching: combining and comparing information from different databases
- (Computer) Profiling: analyzing data to determine characteristics of people most likely to engage in certain behavior
- Opt-in & opt-out: To sign up or unsubscribe from a collection of info.
- Data retention: the continued storage of an organization's data for compliance or business reasons
- 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
- USA Patriot act: eased government access to many kinds of personal info, including financial records, without a court order
- Public Records: Records available to general public (bankruptcy, property, arrest records, salaries of government employees, etc)
- Encryption is a technology, often implemented in software, that transforms data into a form that is meaningless to anyone who might intercept and view it
- Cryptographic software: Hiding data in plain sight: keys
  - o Many Email clients
  - o Secure Messaging
  - o Disk encryption
  - o Anonymity networks
- Audit trial: System keeps track of information about each access (ID of the user that accessed the data, read and write)
- Third-party privacy audits for companies: check for leaks of information, review the company's privacy policy and its compliance with that policy
- Large organizations have a position called chief privacy officer to check the privacy policy
- Free Market View: Response to customer by preference
  - o Freedom of consumers to make voluntary agreements
  - o Diversity of individual tastes and values
  - o Response of the market to consumer preferences

- o Voluntary organizations that provide consumer education
- o Usefulness of Contracts
- o Flaws of regulatory solution
- Consumer Protection View
  - o More stringent requirements, prohibitions on businesses of storing or selling certain type of data
  - o Protect consumers against collection or storage of information that they don't understand
  - o Consumers need protection from their own lack of knowledge, judgement, or interest

Chapter 3 Freedom of Speech
- Cliché: Internet lets us all be publishers
- Restrictions
  - o Children to certain type of information (porn, violence)
  - o Spam
  - o Controversial speech
- Spam: unsolicited bulk email
- Anonymity: hides true identity
- Net Neutrality: Refers to a variety of proposals for restrictions on how telephone and cable companies interact with their broadband customers and set fee for services: Equal treatment for all customers
  - o Common carriers were prohibited from providing own content, and from discrimination based on content or source, called line-sharing (open-access) requirements
- De-regulation: flexibility and market incentives will benefit customers
- Transparency: Fixed and mobile broadband providers must disclose the network management practices, performance characteristics, terms and conditions of their broadband services
- Copyright
- Patents: Protects idea
- Trade marks

Chapter 4 Intellectual Property
- Trademark: is a recognizable name, word, sign (logo), design, or expression which identifies products or services of a particular source from those of others
- Trade secret: a secret device or technique used by a company in manufacturing its products
- Warez: unauthorized copies of software
- Fair use Doctrine
  - o Copyright law and court decisions attempt to define the rights of authors and publishers consistent with two goals
    - Promoting production of useful work
    - Encouraging the use and flow of information
  - o Four factors considered
    1. Purpose and nature of use – commercial or nonprofit purposes
    2. Nature of the copyrighted work
    3. Amount and significance of portion used
    4. Effect of use on potential market or value of the copyright work

- Look and feel: Refers to features such as pull-down menus, windows, icons, and finger movements and specific ways they are used to select or initiate actions
- International Piracy
  - Some countries do not recognize or protect intellectual property
- Digital Rights Management (DRM) collection of techniques that control uses of intellectual property in digital formats
- Anti-circumvention: Prohibit circumventing technological access controls and copy-prevention systems
- Safe Harbor
  - Take down notices they are not in violation
  - Protects Web sites from lawsuits for copyright infringement by users of site
- Free software is an idea advocated and supported by a large, loose-knit group of computer programmers who allow people to copy, use, and modify their software
- GNU project: free programs to download and modify

Chapter 5 Crime
- Hack: clever programming that reflects a high level of skill and that circumvents limits
- Black hat hackers: their activities are destructive, unethical, and usually illegal – we will refer to them as hackers while going forward
- White hat hackers: use their skills to demonstrate system vulnerabilities and improve security – this include cyber security experts warning of potential threats
- Virus: software that attaches itself to other software. Spreads when someone runs an infected program
- Worm: similar to virus but does not require to attach itself to other program to function
- Trojan horse: Malware that appears to be benign but carries malicious component
- Social engineering: Manipulating people to release information or to perform a task which violates security protocol
- Ransomware: Malware that encrypts some or all files on a device and displays a message demanding money (often in bitcoin)
- Spyware: Malware that can monitor and record user activities on a computer or a mobile. This includes logging keystrokes on the keyboard to capture username, password, account number and other info
- Botnet: A group of computers or other devices on the internet that have a virus or malware that communicates with a central host or server controlled by a hacker
- DoS (Denial of Service) attack: An attack in which a botnet overwhelms websites, mail servers, or other internet locations with so many requests for service that normal users cannot access the sites or services.
  - Used to shut down web sites
- Backdoor: Software that allows access to a computer system or device at a future time by bypassing the normal layers of security checks
- Honey pots: web sites that attract hackers to record and study
- Computer forensics (digital forensics) specialists can retrieve evidence from computers, even if the user has deleted files and erased the disks

Identity theft

- The most common way is credit card fraud.
- It impacts the bank and the person whose credit card got stolen. Credit history

- Stuxnet
  - An extremely sophisticated worm
  - Targets a particular type of control system
- Phishing: email
- Smishing: text message
- Vishing: voice phishing

- Pharming: websites (example: virus) fake url
- The ways people get access to your information. Call you and ask for it in a way such that makes the excuse legitimate
- Computer forensics (digital forensics): specialists can retrieve evidence from computers, even if the user has deleted files and erased the disks
- Biometrics: Biological characteristics unique to an individual (example: finger print, eye, face, etc)
- Libel Tourism: traveling to places with strict libel laws in order to sue
- Responsibility-to-prevent-access: Publishers must prevent material or services from being accessed in countries where they are illegal
- Authority-to-prevent-entry: Government of Country A can act within Country A to try to block the entrance of material that is illegal there, but may not apply its laws to the people who create and publish the material, or provide a service, in Country B if it is legal there

Chapter 6 Work
- Has created more high level jobs while decreasing low level jobs. (cashier & programming)
- Telecommuting: Working from home
- Sharing economy: sell products you don't need anymore. (craiglist, ebay, amazon, etc)
- On-demand services: Very quick delivery of products and services
- Gig work: workers work the hours they choose and paid by the job, rather than hourly, e.g. ride sharing Uber, Lyft
- Outsourcing
  - Phenomenon where a company pays another company for services instead of performing those tasks itself
  - A company pays another company to build parts for its products or services instead of performing those tasks itself
- Offshoring
  - The practice of moving business processes or services to another country, especially overseas, to reduce cost
  - The practice of moving business processes or services to another country, especially overseas, to reduce costs
- Inshoring
  - When another company employs thousands of people in your country. (opposite of offshoring)

Chapter 7

- Wisdom of the crowd: ratings by public of website
  - StackOverflow, unreliable info., Manipulate
- Narrowing the information stream
- Abdicating responsibility
  - Rely on computers to judgement
- Evaluating Models
  - Models necessarily involve assumptions and simplifications of reality
- Criticisms of computing technologies
  - Neo-Luddism is a philosophy opposing or skeptical to many forms of modern technology
  - Computers separate humans from nature and destroy the environment
- Trends in Computer Access
  - New technologies only available to the wealthy
  - The time it takes for new technology to make its way into common use is decreasing
  - Cost is not the only factor, ease of use plays a role

Chapter 8 Errors, Failures, and Risks

- Companies usually compete with each other.
  - As a result, there are flaws to their technology
- Therac-25 Radiation Overdoses: a software controlled radiation therapy machine used to treat cancer patients
- Legacy Systems: no one wants to update.
  - No programmers who know how it works bc we all learn the new things
- Preoccupation with failure: always assume something unexpected can go wrong
- Loose structure: it should be easy for a designer or programmer to spear to people in other departments or higher up in the company without going through rigid channels that discourage communication
- To prevent
  - Redundancy – have multiple systems that do the work & compare the results
  - Testing – for all changes. Regardless of size

Chapter 9 Professional Ethics & Responsibilities

The Software Engineer Code (8 principles)
1. Public: Software engineers shall act consistently with the public interest
2. Client and Employer: Software engineers shall act in a manner that is in the best interests of their client and employer consistent with the public interest.
3. Product: Software engineers shall ensure that their products and related modifications meet the highest professional standards possible
4. Judgment: Software engineers shall maintain integrity and independence in their professional judgement
5. Management: Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance

6. Profession: Software engineers shall advance the integrity and reputation of the professional consistent with the public interest
7. Colleagues: Software engineers shall be fair to and supportive of their colleagues
8. Self: Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession