Overview

Introduction

- Characterize cybertechnology and cyberethics
- Professional, philosophical and descriptive perspectives on cyberethics

Ethical Theories

- Grounding moral systems in religion, law or philosophical ethics
- Characteristics of ethical theories: coherent, consistent, comprehensive, and systematic
- Right to distribute proprietary software and other information on the Internet
- Theories: consequence, duty contract, character based
- Apply theories to analyze ethical issues and propose resolutions
Professional Ethics

- Moral responsibility of professionals
- Codes of ethics: ACM, IEEE, SECEPP: pro’s and con’s
- Apply codes to scenarios

Privacy

- aspects of personal privacy: freedom from intrusion and interference, control over flow of personal data
- Why important? supports trust, friendship, security and autonomy
- Data merging, matching, mining
- Personal privacy in public: search engines, online public records
- PET’s anonymity, trustmarks
Security

• What is security: elements are confidentiality, integrity, availability

• Data, system and network security: examples, differences

• Hacking, cyberterrorism, information warfare

• Security and anonymity

• Risk analysis
Cybercrime

- Cybercrime vs. cyberexacerbated and cyberassisted crime
- Piracy, trespass and vandalism: characterize, examples
- Identity theft and corporate espionage
- Combating cybercrime: entrapment, sting operations, keystroke monitoring, packet sniffing, TIA, Patriot Act, encryption, biometric techniques
- Jurisdiction problems for legislation

Compare privacy security and cybercrime
IP

- What is IP? Why protect it?
- Software as IP
- Copyright Law
  - History. SBCETA and DMCA
  - What does it protect?
  - Fair use doctrine
  - First sale doctrine
  - Software piracy vs copyright
  - Jurisdictional issues
- Patents, trademarks and trade secrets: characterize, examples
- Philosophical foundations: labor, utilitarianism, personality theories
- FSF and Open Source: GPL, similarities and differences