Computing Laws and Cases Study Guide

CS 301 Study supplement for Exam 2

Chapter 2:

Laws

- **Fourth Amendment:** People are protected against unreasonable searches of: homes, persons, papers, and effects.
- **Privacy Act of 1974:** establishes a Code of Fair Information Practice that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies
- **E- Government Act of 2002:** improved the management and promotion of electronic government services and processes and established a framework of measures that require using Internet-based information technology to improve citizen access to government information and services
- **REAL ID Act:** set forth requirements for state driver's licenses and ID cards to be accepted by the federal government for "official purposes".
- **Electronic Communications Privacy Act:** extended government restrictions on wiretaps to include transmissions of electron data by computer.
- **PATRIOT Act:** aimed at deterring and punishing terrorist acts in the United States and around the world. It enhanced law enforcement investigatory tools.
- **Communications Assistance for Law Enforcement Act:** Enhanced the ability of law enforcement agencies to conduct electronic surveillance by requiring private communication companies to have built-in surveillance capabilities.

Cases

- **Olmstead v. United States:** The Supreme Court ruled that wiretapped phone conversations obtained without a warrant did not violate the Fourth or Fifth Amendment
- **Katz v. United States:** Overruled the decision of Olmstead v. United States. Redefined the unreasonable search and seizure clause of the Fourth Amendment to include intrusion with technology as a search. Also extended the Fourth Amendment to areas where a person has a "reasonable expectation of privacy".
- **Smith v. Maryland:** The use of a pen register did not constitute a violation of the legitimate expectation of privacy, since the numbers would be available to and recorded by the phone company anyway.
- **Kyllo v. United States:** use of advanced technology, such as thermal imaging, from a public vantage point constituted a search and thus required a warrant.
- **Jones v. United States:** installing a GPS tracking device on a vehicle constitutes a search under the Fourth Amendment and thus requires a warrant.

Chapter 3:

Laws

- **Telecommunications Act of 1996:** No computer service provider/user can be treated as the publisher or speaker of information provided by another information content provider
- **Communications Decency Act (CDA) of 1996:** Making obscene/indecent communication available with anyone under 18 is illegal. Ruled unconstitutional
- **Child Online Protection Act (COPA) in 1998:** Adults required to provide identification to view material that is inappropriate for minors. Ruled unconstitutional
- **Children's Internet Protection Act (CIPA) of 2000:** Required libraries and schools to use filter software on Internet terminals. Ruled unconstitutional
- **CAN-SPAM Act of 2003:** Regulates commercial spam (Mail header information and valid return address must be included) (Rules for generating emailing lists, labeling advertising messages, and providing opt-out features)

Chapter 4:

Laws

- **U.S. Copyright Law (Title 17 of the U.S. Code) first passed 1790:** Copyright holders have the exclusive rights to perform, distribute, display, and make copies of their work (or produce derivative works)
- **No Electronic Theft Act of 1997:** illegal to knowingly infringe copyright for works worth more than $1000, even if there is no commercial gain
- **Digital Millennium Copyright Act (DMCA) in 1998:** Circumventing DRM is illegal, and websites are not liable for the content of their users, provided they moderate it

Cases

- **Sony vs. Universal City Studios in 1984:** Recording a video for later viewing is considered "fair use" of the work
- **Sega Enterprises, Ltd. v. Accolade, Inc:** Reverse engineering software is fair use
- **Atari Games v. Nintendo:** Making copies of a program to reverse engineer is is fair use
- **Sony v. Connectix Corporation:** Emulation of other systems' BIOS is fair use
- **RIAA v. Napster:** Napster "knowingly encourages and assists in the infringement of copyrights" because they served to benefit from giving users access to free music sharing
- **MGM v. Grokster:** Businesses that encourage copyright infringement are not legal
- **RIAA v. Diamond Multimedia Systems in 1998:** Music players allow for fair use of works
- **Pirate Bay Case (Sweden) in 2009:** Helping users access unauthorized copyrighted material is illegal
- **Kelly v. Arriba Soft:** Using images for thumbnails in search results is not infringement
- **Field v. Google:** Caching web pages is fair use
- **KSR v. Teleflex in 2007:** Broadened what "obvious" means for rejecting patents
- **Bilski v. Kappos in 2010:** Patent cannot be given for abstract ideas

Chapter 5:

Laws

- **Computer Fraud and Abuse Act:** hacking federal computers, financial systems, and interstate systems or international systems under federal jurisdiction
- **US Patriot Act:** Raised hacking offence to 10 years in jail minimum. Expanded the definition of hacking
- **Unlawful Internet Gambling Act:** prohibits credit card and online-payment companies from processing transactions between bettors and gambling sites
- **Defamation Law:** we can sue a person, business, or organization for saying something false and damaging to our reputations in print or in other media such as TV or the Web
- **SPEECH Act of 2010:** foreign libel judgements are unenforceable in the U.S. if they would violate the First Amendment

Cases

- **Sony vs. George Hotz:** Hotz showed how to use pirated apps and games on the Sony PS3. Led to retaliation attack on PlayStation Network

Chapter 6:

Laws

- **Electronic Communications Privacy Act (ECPA):** prohibits interception of email and reading of stored email without a court order, with the exception for businesses and employee email. Previously covered in Chapter 2
- **Computer Fraud and Abuse Act (CFAA):** hacking federal computers, financial systems, and interstate systems or international systems under federal jurisdiction.Previously covered in Chapter 5