CS4984
Computer Crime & Open Source

Ross Dannenberg
Rdannenberg@bannerwitcoff.com
(202) 824-3153
Computer Crime

Specific Federal Statutes

- Computer Fraud & Abuse Act (CFAA)
- Electronic Communications Privacy Act (ECPA)
- Encryption Export Control Act (EECA)
- International Emergency Economic Power Act (IEEPA)
- Economic Espionage Act (EEA)
Computer Crime

Specific Federal Statutes (cont’d)

• Criminal Trademark statutes
• Criminal Copyright statutes
• Patent Forgery statute
• Identity Theft and Assumption Deterrence Act (ITADA)
• Government Confidential Information Act
• National Defense Information Act (NDIA)
Computer Crime

General Federal Statutes

- Obscenity and Child Pornography
- Wire Fraud, Mail Fraud
- Securities Fraud
- National Stolen Property Act
- RICO
- Money Laundering statute
- Prohibited Financial Transactions statute
- Conspiracy, Aiding, & Abetting
Computer Fraud & Abuse Act

• Protected computer = computer used in interstate communication
• Prohibits:
  – Unauthorized disclosure of sensitive national defense, foreign relations, or nuclear technology information obtained by unauthorized access to protected computer.
  – Obtaining information from a protected computer through unauthorized access
  – Unauthorized access to any federal gov’t computer
  – Furthering a fraud through unauthorized access to a protected computer
Computer Fraud & Abuse Act

• Prohibited acts
  – Damaging a protected computer
  – Trafficking in passwords affecting interstate commerce or federal gov’t computer
  – Making a threat to damage a protected computer in order to extort money of another item of value.

• USA PATRIOT Act
  – Adds foreign computers that affect U.S. interstate communications
  – Lighter “damage” requirements
  – Extended jail terms
Electronic Communications Privacy Act

- Expands the Wiretap Act’s prohibitions to include interception of electronic communication
- Prohibits access to a facility through which an electronic communication service is provided
Electronic Communications Privacy Act (cont’d)

• USA PATRIOT Act
  – Included “voicemail” in def’n of electronic communication
  – Gov’t can intercept comm. from computer trespasser with permission of owner of victim computer
  – Easier for gov’t to obtain personal info from computer providers
Trafficking in Counterfeit Goods & Services

- Prohibits
  - Trafficking in goods or services bearing counterfeit trademarks
  - Must be intentional or knowingly
  - Individual Penalties
    - Up to $5,000,000 fine; 20 years in prison
  - Non-Individual Penalties (i.e., an organization)
    - Up to $15,000,000 fine

- Also a crime to traffic in counterfeit labels and computer program documentation and packaging.
Criminal Copyright Infringement

• Prohibited conduct
  – Willful copyright infringement
  – For purposes of commercial advantage or private financial gain, or value $1,000 (within 180 day period)

• Damages
  – $$$ based on number of infringing copies and retail value of those copies (up to $500,000); and/or
  – Jail (up to 10 years)
Virginia Statutes

• Virginia Computer Crimes Act
  – Protected Devices:
    • Any electronic, magnetic, optical, hydraulic, or organic device
  – Prohibited Acts:
    • Computer fraud
    • Computer trespass
    • Computer invasion of privacy
    • Theft of computer services
    • Personal trespass by computer
    • Harassment by computer
    • Computer forgery
    • Encryption in a criminal activity
Software Licensing

• Shrinkwrap
• Click-wrap
• Open Source issues
Shrinkwrap and Clickwrap Agreements

• Common provisions
  – scope of license/restrictions on use (noncommercial) -- ProCD case
  – limitations on use of data (screen scrapers, e-mail harvesters)
  – anti-reverse engineering clauses -- Bowers case
  – limitations on copying/distributing/linking/framing
  – disclaimers (warranty of fitness/merchantability/etc)
  – anti-disparagement provisions
  – arbitration clauses
Shrinkwrap and Clickwrap Agreements (cont’d)

• Why use them?
  – extra layer of protection beyond copyright/patent/trade secret
  – protections not available under other theories (reverse engineering; noncopyrightable subject matter; waiver of patent/copyright defenses)
  – can select venue for arbitrations/litigation
  – avoid copyright "first sale" doctrine
Shrinkwrap and Clickwrap Agreements (cont’d)

• Enforcement issues
  – Validity of assent (must give notice prior to downloading/executing)
    • Specht v. Netscape Communications, 306 F.3d 17 (2d Cir. 2002) (buyer downloaded software without ever looking at license terms: no assent to terms)
  – Recordkeeping/proof problems (terms, dates, procedures, etc)
  – Unconscionability (agreements not to publish/compete/test)
Shrinkwrap and Clickwrap Agreements (cont’d)

• Are there any limits?
  – "By opening this can of soda, you agree not to reverse-engineer the formula."
  – "By using this software, you agree not to sue us for any reason."
  – "If you return this product to us, you agree not to use any competitor's product."
  – "By opening this book, you agree not to write an unfavorable review of it."

• UCITA (MD and VA only) may affect enforcement
Copyright Preemption

• Are Shrinkwrap/Clickwrap Agreements Preempted?
• A claim is preempted if:
  – Work is "fixed" in tangible medium (disk, paper, etc)
  – Work is a copyrightable "work of authorship"
  – Rights asserted under claim are equivalent to rights provided by copyright act (reproducing, adapting, distributing, performing, etc).
Copyright Preemption (cont’d)

• Are shrinkwrap or clickwrap agreements preempted by copyright act?
  – Agreement to not copy: analogous to copyright reproduction right
  – Agreement to not further distribute: analogous to copyright distribution right
  – Agreement to not use uncopyrightable parts of work: analogous to fair use defense
  – Other terms: must look at individually
Copyright Preemption (cont’d)

  - Shrinkwrap software agreement: "no copying; no reverse engineering allowed"
  - Is agreement preempted? Baystate argued:
    - anti-copying provision was equivalent to reproduction right
    - anti-reverse engineering provision conflicted with fair use defense
Bowers v. Baystate (cont’d)

• Court said:
  – Contract rights are individual rights; copyrights are against the world
  – Contracts have offer, acceptance, consideration, breach
  – Reverse engineering provision: does not conflict with fair use defense
  – OK to waive defense of fair use in contract
  – DMCA has limited "fair use" reverse engineering provision

• Lesson learned: OK to enforce anti-reverse engineering clause (very broad)
Open Source Licensing
Issues: What a Mess!

• General Public License (GPL) and Free Software Foundation (www.gnu.org)
• Risks/Problems with the GPL
• Linux: relies on the GPL
• SCO v. IBM: testing the GPL
O-STEP – An Alternative to Open Source

• Open Source Threshold Escrow Program
  – An intermediary between proprietary and open source models

• O-STEP Escrow Agreement
  – Escrow software with the Center of Open Source & Government
  – When sales threshold met, source code is released to open source community
    • Sales threshold set by company?
    • What about new versions of software?
Review for Exam

Any Questions?