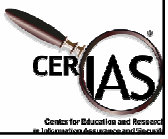
PURDUE
UNIVERSITY

CS526: Information Security
Chris Clifton

November 30, 2004

CyberLaw



Computer Law: Why?

- Theft
  - of Computers
  - of Information
- Use of computers in crime
- Purpose of laws:
  - Define right/wrong
  - Determine penalties for wrongdoing
  - Establish means to protect against wrongdoing

Range of Issues

- Use of computers in other crimes
  - Computer-specific laws
  - Law enforcement in a computer age
- Computer-specific crimes
  - Network-based attacks
  - Spam
- Use of cryptography
  - Export control
  - Digital signatures
- Legal issues *changed* by computers
  - Copyright
  - Privacy

Applicable Pre-Electronic Laws

- Theft of Information
  - Trade secrets
  - Trademark
  - Copyright
  - Patent
- Theft of Computing Services
  - Trespass to Chattels
- Use of Computer in Crime
  - Already punishment for the crime…

Why do we need more?

- Civil vs. Criminal
  - Trespass to chattels primarily civil
  - Lack of criminal penalties (no more debtor's prison…)
- Laws unclear where computers concerned
  - Software patent
  - Fair use in copyright
- Standards of proof
  - Easier to prove a computer used to (attempt to) commit a crime than to prove the crime itself?

So what are the laws?

- Computer Fraud and Abuse Act
  - TITLE 18 > PART I > CHAPTER 47 > § 1030
  - Fraud and related activity in connection with computers
- Electronic Communications Protection Act
  - TITLE 18 > PART I > CHAPTER 121
  - Governs misuse of information
- Digital Millenium Copyright Act
- Computer Security Act
  - Directs NIST to establish standards for securing Federal computer systems

Computer Fraud and Abuse Act

- TITLE 18 > PART I > CHAPTER 47 > § 1030
- Applies to "Protected Computers"
  - Exclusively for the use of a financial institution or the U.S. Government (or when offence affects such use, if not exclusive)
  - Used in interstate or foreign commerce or communication
- Liability on anyone who (to a "protected computer") who does or attempts to
  - Intentionally accesses without or in excess of authorization to steal more than $5000 per year
  - Sends command/program that causes damage
  - Traffics in passwords or other means to access
  - Communication threatening to damage with intent to extort
  - Any damage to information or access that results in physical injury
- Imposes both criminal and civil liability
  - Criminal penalties vary, typically 1-10 years first offence, 10-20 subsequent, and/or fines

Why Limits on "Protected Computer"

- A little U.S. History…
  - Primary power rests with the states
  - Generally federal government has no right to regulate what goes on
  - Some exceptions, key one is "Interstate Commerce"
- Result: Federal laws only apply in specific instances
  - State law covers the rest
- But "Interstate Commerce" can cover almost anything

Example State Laws

- Indiana
- California

Electronic Communications Protection Act

- TITLE 18 > PART I > CHAPTER 121
- Wiretap Act
  - Criminalizes attempts to intercept or disclose intercepted "electronic communications"
- Stored Communications Act
  - Extends to stored, rather than intercepted, communications
  - "electronic communications system" means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications
- Generally consent of *one party* sufficient to intercept/disclose communications

Digital Millenium Copyright Act

- Attempts to bring copyright into digital age
  - Copying easier
  - Copy indistinguishable from original
- Key provision: proscribes devices or services that circumvent copy protection that:
  - are primarily designed or produced to circumvent;
  - have only limited commercially significant purpose or use other than to circumvent; or
  - are marketed for use in circumventing.
- Some exceptions
  - Libraries (for fair use purposes)
  - Reverse engineering (under license) to achieve interoperability
  - Encryption research
  - Protection of minors
  - Protecting personal privacy
  - Security testing

Computer Security Act

- Directs NIST to establish standards for securing Federal computer systems
  - Doesn't include DoD / Intelligence
  - Does include systems operated by private contractors for the government
- Covers "standards" in a broad sense
  - Cryptography
  - Protocols
  - Training
  - Validation/testing
  - Gives NSA some responsibility for technical development
- Importance to researchers: Includes authority / responsibility for R&D
- 2002: Federal Information Security Management Act
  - Gives Office of Management and Budget responsibility ot oversee NIST, NSA, DoD computer security efforts

Related (Not computer-specific)

- Economic Espionage Act
  - Criminalizes theft of trade secrets for gain
- Privacy laws
  - European Union
  - US HIPAA rules (www.hipaadvisory.com)
  - Many others: (www.privacyexchange.org)
  - Often control transborder use of data
  - Focus on intent
    - Limited guidance on implementation

Regulatory Constraints: Privacy Rules

- Primarily national laws
  - European Union: EC95/46
  - US HIPAA rules (www.hipaadvisory.com)
  - Many others: (www.privacyexchange.org)
- Often control transborder use of data
- Focus on intent
  - Limited guidance on implementation

European Union Data Protection Directives

- Directive 95/46/EC
  - Passed European Parliament 24 October 1995
  - Goal is to ensure free flow of information
    - *Must preserve privacy needs of member states*
  - Effective October 1998
- Effect
  - Provides guidelines for member state legislation
    - Not directly enforceable
  - Forbids sharing data with states that don't protect privacy
    - Non-member state must provide adequate protection,
    - Sharing must be for "allowed use", or
    - Contracts ensure adequate protection
  - US "Safe Harbor" rules provide means of sharing (July 2000)
    - Adequate protection
    - But voluntary compliance
- Enforcement is happening
  - Microsoft under investigation for Passport (May 2002)
  - Already fined by Spanish Authorities (2001)

EU 95/46/EC: Meeting the Rules

- Personal data is any information that can be traced directly *or indirectly* to a specific person
- Use allowed if:
  - Unambiguous consent given
  - Required to perform contract with subject
  - Legally required
  - Necessary to protect vital interests of subject
  - In the public interest, or
  - Necessary for legitimate interests of processor and doesn't violate privacy

EU 95/46/EC: Meeting the Rules

- Some uses specifically proscribed
  - Can't reveal racial/ethnic origin, political/religious beliefs, trade union membership, health/sex life
- Must make data available to subject
  - Allowed to object to such use
  - Must give advance notice / right to refuse direct marketing use
- Limits use for automated decisions (e.g., creditworthiness)
  - Person can opt-out of automated decision making
  - Onus on processor to show use is legitimate and safeguards in place to protect person's interests
  - Logic involved in decisions must be available to affected person

europa.eu.int/comm/internal_market/privacy/index_en.htm

US Healthcare Information Portability and Accountability Act (HIPAA)

- Governs use of patient information
  - Goal is to protect the patient
  - Basic idea: Disclosure okay if anonymity preserved
- Regulations focus on outcome
  - A covered entity may not use or disclose protected health information, except as permitted or required…
    - To individual
    - For treatment (generally requires consent)
    - To public health / legal authorities
  - Use permitted where "there is no reasonable basis to believe that the information can be used to identify an individual"
- Safe Harbor Rules
  - Data presumed not identifiable if 19 identifiers removed (§ 164.514(b)(2)), e.g.:
    - Name, location smaller than 3 digit postal code, dates finer than year, identifying numbers
  - Shown not to be sufficient (Sweeney)
  - Also not necessary

Moral: Get Involved in the Regulatory Process!