

Laws

- ❖ *DigitalSherlock.com | SafeHack.com*
- ❖ *Date: 2005/05/27*
- ❖ *Document Name: laws.pdf*
- ❖ *GNU Free Documentation License*
- ❖ *Version 1.00, 2005-05-27*
- ❖ *Copyright © 2005 Adonis, MSc, Eng, CISSP, Security+, CEH, GSec, MCSE, etc.*
- ❖ *Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation.*

❖ Security Related Laws

- **1934 Federal Communications Act**
 - The Act prohibits any party involved in sending such communications from divulging or publishing anything having to do with its contents.
 - It makes an exception and permits disclosure if the court has issued a legitimate subpoena.
 - Any materials gathered through an illegal wiretap is inadmissible and may not be introduced as evidence in federal courts.
- **1970 U.S Fair Credit Reporting Act**
 - Covers Consumer reporting agencies
 - Requires consumer reporting and credit agencies to disclose information in their files to affected consumers.
- **1970 U.S Racketeer Influenced & Corrupt Organization (RICO)**
 - Addresses Criminal & Civil crimes
 - Mail fraud
 - Security fraud
 - Fraud using a computer
- **1973 U.S. Code of Fair Information Practices**
 - Personal record keeping
- **1974 Federal Privacy Act**
 - Applies to records and documents maintained by the federal government
 - Addressed the fact that there are many technological problems relating to privacy of information using technology.
 - Disclosure of personal information is limited to only authorized persons
 - Provide safeguards for an individual against an invasion of privacy.
 - Under the Privacy Act, individuals decide which records kept by a federal agency or bureau are important to them.
 - They can insist that these data be used only for the purposes for which the information was collected.
 - The records must be accurate, Relevant, Timely, and Complete
 - Safeguard are required to ensure security and confidentiality of records
 - They may correct mistakes or add important details when necessary.
 - A record is information about a person
 - Education
 - Medical History
 - Financial History
 - Criminal History
 - Employment History

- It does not apply to congressional, judiciary or territorial subdivisions
- **1980 OECD**
 - Organization for Economic Cooperation & Development
 - Deal with data collection limitations
 - Quality of the data
 - Purpose of data collection
 - Limitation on data use
 - Information security safeguards
 - Openness
- **1984 U.S. Medical Computer Act**
 - Deal with illegal access to medical records by phone or data networks
 - Was a result of the “414 gang” who broke into a New York Hospital’s computer.
 - Focuses on protecting information that uses computers and telecommunication devices that access medical records.
- **1984 Comprehensive Crime Control Act**
 - US Federal Act
 - Focused attention on the need to fight computer related crimes.
- **1984 First U.S. Federal Computer Crime Law Passed**
 - Covered classified defense or foreign relations information
 - Records of financial institutions
 - Unauthorized access or access of authorization
- **1986 (Amended in 1996) U.S. Computer Fraud & Abuse Act**
 - Clarified the 1984 Law
 - Illegally using federal computers is a fraud
 - Altering damaging federal information
 - When preventing the use (e.g DoS) of federal computer caused a loss > 1000 \$
 - Trafficking passwords that allow unauthorized access to federal computers
- **1987 U.S. Computer Security Act**
 - The act states that the security and privacy of federal computer systems are in the public interest.
 - The Act requires that each U.S. Federal agency to provide its employees with training in computer security awareness
 - Identify sensitive systems
 - Develop a security plan for those systems
 - Consider Sensitive But Unclassified SBU
 - Consider Sensitive Unclassified Information SUI
 - This act give NIST and NSA the responsibility for information security
 - NSA is responsible for cryptography
- **1990 United Kingdom Computer Misuse Act**
 - Defines computer related criminal offences
- **1991 U.S. Federal Sentencing Guidelines**
 - Provides punishment guidelines for those found guilty of breaking federal Law
 - Threat the unauthorized possession of information
 - Address both individuals and organizations
 - Make the degree of Punshiment funtion of due diligence

- **Invoke Prudent man rule**
 - senior management can be charged to pay up to \$290 million
- **The law that made it easier for judges to send corporate officers to jail for various white collar crimes**
- **1992 OECD Guidelines to serve as a Total Security Framework**
 - Framework for Laws
 - Framework for Policies
 - Framework for technical & administrative measure
 - Framework for education
- **1994 U.S. Communications Assistance for Law Enforcement Act**
 - Requires all communications carriers to make WIRETAPS possible
- **1994 U.S. Computer Abuse Amendments Act**
 - Changed the federal interest computer to computer used in interstate commerce or communications
 - Covers viruses & worms
 - Covers intentional/reckless damage
 - Limited imprisonment for UNintentional damage to one year
 - Provides civil action to obtain compensatory damages
- **1995 Council Directive (Law) on Data Protection for the European Union (EU)**
 - Declare that each EU nation must have protections similar to thoses in OECD guidelines
- **1995 BS 17799**
 - BS 17799 was first published in February 1995
 - Comprehensive set of controls comprising best practices in information security.
 - Intended to serve as a single reference point for identifying a range of controls needed for most situations where information systems are used in industry and commerce, and to be used by large, medium and small organizations.
 - It was significantly revised and improved in May 1999 and became ISO17799 in December 2000.
 - It is contain major sections
 - 1.Business Continuity
 - 2.Systems Access Control
 - 3.System Development and Maintenance
 - 4.Physical and Environmental Safety
 - 5.Compliance
 - 6.Personnel Security
 - 7.Security Organization
 - 8.Computer and Network Management
 - 9.Asset Classification
 - 10.Security Policy
- **1996 Computer Fraud Act**
 - Is the primary federal anti-hacking statue
 - It categorizes seven forms of activity as federal crimes
- **1996 U.S. Economic Espionage Act**
 - Addresses industrial and corporate espionage

- Which made theft of “trade secrets” a federal felony.
- 15 years in prison and \$10 million in fines
- **1996 U.S. HIPAA Health Insurance & Portability Accountability Act**
 - Address the issues of personal health care information privacy
 - Address Health plan portability in the U.S
- **1996 U.S. National Information Infrastructure Protection Act**
 - It amended the computer Fraud & abuse act
 - It helped protect all U.S. government computers, referred to computers used in foreign commerce and punishes by felony anyone who causes damage.
 - Codified 18 U.S.C. § 1030
- **1999 Anticybersquatting Consumer Protection Act**
 - This act made it easier for individuals and companies to take over domain names that are confusingly similar to their names or valid trademarks.
 - One portion of this Act related to famous individuals.
 - This portion allows individuals to file a civil action against anyone who registers their name as a second level domain name for the purpose of selling the domain name for a profit.
- **2001 USA Patriot Act**
 - On October 26, 2001, US President George W. Bush signed
 - Providing Appropriate Tools Required to Intercept and Obstruct Terrorism”
 - Police can sneak into someone’s house or office, search the contents, and leave without ever telling the owner. This would be supervised by a court, and the notification of the surreptitious search "may be delayed" indefinitely. (Section 213)
 - Any U.S. attorney or state attorney general can order the installation of the FBI's Carnivore surveillance system and record addresses of Web pages visited and e-mail correspondents -- without going to a judge. Previously, there were stiffer legal restrictions on Carnivore and other Internet surveillance techniques. (Section 216)
 - Any American "with intent to defraud" who scans in an image of a foreign currency note or e-mails or transmits such an image will go to jail for up to 20 years. (Section 375)
 - An accused terrorist who is a foreign citizen and who cannot be deported can be held for an unspecified series of "periods of up to six months" with the attorney general's approval. (Section 412)
 - Biometric technology, such as fingerprint readers or iris scanners, will become part of an "integrated entry and exit data system" with the identities of visa holders who hope to enter the U.S. (Section 414)
 - Any Internet provider or telephone company must turn over customer information, including phone numbers called -- no court order required -- if the FBI claims the "records sought are relevant to an authorized investigation to protect against international terrorism." The company contacted may not "disclose to any person" that the FBI is doing an investigation. (Section 505)
 - Credit reporting firms like Equifax must disclose to the FBI any information that agents request in connection with a terrorist investigation -- without police needing to seek a court order first. Current law permits this only in espionage cases. (Section 505)
 - The current definition of terrorism is radically expanded to include biochemical attacks and computer hacking. Some current computer crimes -- such as hacking a U.S. government system or breaking into and damaging any Internet-connected computer -- are covered. (Section 808)
 - A new crime of "cyberterrorism" is added, which covers hacking attempts causing

damage "aggregating at least \$5,000 in value" in one year, any damage to medical equipment or "physical injury to any person." Prison terms range between five and 20 years. (Section 814)

- New computer forensics labs will be created to inspect "seized or intercepted computer evidence relating to criminal activity (including cyberterrorism)" and to train federal agents. (Section 816)

➤ **RFC 1087**

- RFC 1087 states that access to and use of the Internet is a privilege

❖ **Common Law System Categories**

➤ **Civil Law**

- Also called Tort
- Deals with wrongs against individuals or companies that result in damages or loss
- Laws about a wrong inflicted upon an individual or organization
- Punishment **CANNOT** include imprisonment but it can include financial
- Award mechanisms
 - A.) Statutory Damages
 - B.) Punitive Damages
 - C.) Compensatory Damages

➤ **Criminal Law**

- Is used when an individual's conduct violates the government's laws, which have been developed to protect the public
- Laws about individual conduct that violates government laws
- Punishment can include financial penalties & imprisonment
- Jail sentences are commonly the punishment

➤ **Administrative Regulatory Law**

- Deals with regulatory standards that regulate performance and conduct
- Government agencies create these standards
- Standards of performance expected by government agencies from industries
- Punishment can include financial penalties AND/OR imprisonment

➤ **Intellectual Property Law**

- **Copyright**
 - Protects Original works of authorship. Distribution, reproduction etc
 - Can be applied to Software & Databases
 - Protects the expression of the idea of the resource NOT the idea
 - The Copyright Act grants five rights to owner
 - ◆ - the right to reproduce the copyrighted work;
 - ◆ - the right to prepare derivative works based upon the work;
 - ◆ - the right to distribute copies of the work to the public;
 - ◆ - the right to perform the copyrighted work publicly; and
 - ◆ - the right to display the copyrighted work publicly.
 - ◆ The right to profit cannot be granted.
- **Trade Secret**
 - Secures & maintains the confidentiality of proprietary technical or business information
 - The resource that is claimed to be a trade secret must be confidential and protected with certain security precautions and actions.
- **TradeMark**
 - Protect a word, name, symbol, sound, shape, colour, device or combination of these

- **Patent**
 - Provide the owner with a legally enforceable right
 - Patent period 17 Years in USA
 - Are given to individuals or companies to grant the owner legal ownership and enable the owner to exclude others from using and copying the innovation covered by the patent.

➤ **Information Privacy Law**

- (EU) European Union
- U.S Privacy Regulations

❖ **Fallacy (A false notion)**

➤ **The Computer Game Fallacy-**

- This fallacy is the view that what you do with a computer is not wrong, it is like a game.
- These same hackers would not consider using this defense if they jumped a fence and walked into someone's home.

➤ **The Law Abiding Citizen Fallacy-**

- As long as it does not break a law I am OK.
- I can write a virus and allow people to have it, this is legal,
- It can often be confusing to decide what the allowed behaviors are and the minimums for those behaviors.

➤ **The Candy from a Baby Fallacy-**

- Many computer crimes are very easy to do so they don't really seem wrong.
- For example, someone may make a copy of software that he does not own and use for their personal use.

➤ **The Hacker Fallacy-**

- This is based on the idea that they are just doing it for the experience or to learn.
- This does not make it right.
- I may want to learn about locks, but that does not mean I would go around picking the neighbors locks.

➤ **The Free Information Fallacy-**

- This is based upon a common notion that if information had a mind of its own, it would want to be free.

❖ **Privacy Related Laws**

➤ **1974 U.S. Privacy Act**

- Applies to federal agencies
- Protection of information about individuals

➤ **1996 U.S. HIPAA**

- Health Insurance & Portability Accountability Act
- Addresses the issues of personal health care information privacy
- Address Health plan portability in the U.S

➤ **1986 U.S. Electronic Communications Privacy Act**

- Prohibits Eavesdropping
- Prohibits interception of message contents

❖ **Import Export Laws**

- There is not restrictions on domestic use in USA pertaining to encryption products

- **American companies can export any encryption product to any end user in the European Union and eight other trading partners**
- **BXA Bureau of Export Administration governs exportation of encryption**