Jurisdictions, Laws and Authorities related to IA

Professor Stephen S. Yau

Spring 2014

IA Related Laws

- **Laws** are rules that ***mandate*** or ***prohibit*** certain behavior in society
  - Different from **ethics**, which define ***socially acceptable behaviors***
  - Laws carry the sanctions of a governing authority and ethics do not

IA Relevant U.S. Laws

- General Computer Crime Laws
- U.S.A. Patriot Act
- Privacy related Laws
- Export and Espionage Laws
- U.S. Copyright Laws
- Freedom of Information Act

• • •

General Computer Crime Laws

- ***Computer Fraud and Abuse Act of 1986 (CFA Act)***
  - The cornerstone of many computer-related federal laws and enforcement efforts
  - Defines and formalizes laws to ***counter threats from computer-related acts and offenses***
  - Amended in October 1996 by ***National Information Infrastructure Protection Act of 1996***
  - Amended on October 26, 2001 by the ***U.S.A. PATRIOT anti-terrorism legislation***

*http://www.panix.com/~eck/computer-fraud-act.html

General Computer Crime Laws (cont.)

- ***National Information Infrastructure Protection Act (NIIPA) of 1996***
  - Categorized crimes based on ***defendant's authority to access federal computer and criminal intent***
  - Increased penalties for selected crimes,
    - For example , improper access or threat to privacy from those in which the defendant uses access for pernicious purposes. Making such conduct a felony, rather than a misdemeanor, if it is committed for financial gain, or results in gathering of information worth more than $5,000.

*http://ecommerce.hostip.info/pages/769/National-Information-Infrastructure-Protection-Act-NIIPA-1996.html (1996)

*http://epic.org/security/1996_computer_law.html (1996)

General Computer Crime Laws (cont.)

- ***Computer Security Act of 1987***
  - One of the first attempts to ***protect federal computer systems by establishing minimum acceptable security practices***
  - Assigned NIST to develop minimum acceptable practices with the help of NSA
  - Requires establishment of security policies for federal computer systems that contain sensitive information.
  - Mandatory security awareness training for federal employees that use those systems.
  - Superseded by the ***Federal Information Security Management Act of 2002 (FISMA)***

*** http://en.wikipedia.org/wiki/Computer_Security_Act_of_1987**

http://epic.org/crypto/csa/csa.html

Federal Information Security Management Act of 2002 (FISMA)

- Recognizes the importance of information security to economic and national security interests of the US.
- Requires each federal agency to develop, document and implement an agency-wide program to provide ***security for the information and information systems***, including those provided or managed by another agencies, contractors or other sources
- Imposes a mandatory ***annual audit and report*** to OMB.
- Emphasizes a ***risk-based policy for cost-effective security***

***http://en.wikipedia.org/wiki/Federal_Information_Security_Management_Act_of_2002**

http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

The Patriot Act

- ***U.S.A. Patriot Act***
  - ***Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*** (Public Law 107-56), known as the ***USA PATRIOT Act*** or simply the ***Patriot Act***
  - Signed on October 26, 2001
  - The Act modified a wide range of existing laws to expand the authority of U.S. law enforcement agencies for the stated purpose of ***fighting terrorism*** in the United States and abroad

*** http://en.wikipedia.org/wiki/USA_PATRIOT_Act**

The Patriot Act (cont.)

- Title I: ***Enhancing Domestic Security against Terrorism***
- Title II: ***Enhanced Surveillance Procedures***
- Title III: ***International money laundering abatement and anti-terrorist financing act*** of 2001
- Title IV: ***Protecting the border***
- Title V: ***Removing obstacles to investigating terrorism***

The Patriot Act (cont.)

- Title VI: ***Providing aid to public safety officers and their families*** when the officers are injured or killed in line of duty
- Title VII: ***Increased information sharing for critical infrastructure protection***
- Title VIII: ***Strengthening the criminal laws against terrorism***
- Title IX: ***Improved intelligence***
- Title X: Miscellaneous

The Patriot Act (cont.)

- ***Key acts changed by The PATRIOT Act***
  - ***Foreign Intelligence Surveillance Act of 1978 (FISA)***
    - allow government agencies to gather "foreign intelligence information" from both U.S. and non-U.S. citizens
  - ***Electronic Communications Privacy Act of 1986 (ECPA)***
    - allow surveillance of public network communication, including emails and web sites.
  - ***Money Laundering Control Act of 1986***
    - strengthen U.S. measures to prevent, detect and prosecute international money laundering and financing of terrorism
  - ***Bank Secrecy Act (BSA)***
    - make it harder for money launderers to operate and easier for law enforcement and regulatory agencies to police money laundering operations
  - ***Immigration and Nationality Act.***
    - give more law enforcement and investigative power to US Attorney General and to Immigration and Naturalization Service (INS).

Privacy Related Laws

- ***The Federal Privacy Act of 1974***
  - Governs federal agency use of ***personal information***
    - Ensure that ***government agencies*** protect the privacy of individuals' and businesses' information
    - Hold those agencies responsible if any portion of the information is released without permission

* http://www.justice.gov/opcl/privacyact1974.htm

Privacy Related Laws (cont.)

- ***Electronic Communications Privacy Act of 1986***
  - Also referred to as the ***Federal Wiretapping Act***
  - Regulates ***interception and disclosure of electronic information***, including wire, electronic, and oral communications

  * http://cpsr.org/issues/privacy/ecpa86/ (1986)

  - In 2001, changed to allow surveillance of public network communication, including emails and web sites.

Privacy Related Laws (cont.)

- ***Health Insurance Portability and Accountability Act of 1996 (HIPAA)***
  - Regulates collection, storage, and transmission of ***sensitive personal health care information***
  - Protects confidentiality and security of health-care data by establishing and enforcing standards and by ***standardizing electronic data interchange***

Privacy Related Laws (cont.)

- ***HIPAA (cont.)***
  - Five fundamental principles:
    - Consumer control of medical information
    - Boundaries on use of medical information
    - Accountability for privacy of private information
    - Balance of public responsibility for use of medical information for the greater good measured against impact to the individual
    - Security of health information

***http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act**

***http://www.cms.gov/HIPAAGenInfo/Downloads/HIPAALaw.pdf**

Privacy Related Laws (cont.)

- ***Gramm-Leach-Bliley Act of 1999 (GLB)***
  - Allow mergers of banks, insurance, and securities firms to form corporations with financial services
  - Requires ***all financial institutions*** to ***disclose their privacy policies on the sharing of nonpublic personal information***. Also requires ***due notice to customers so that they can request that their information not be shared with third parties***
  - Significant impact on the privacy of personal information used by these industries

* http://www.senate.gov/~banking/conf/ (1999)

Privacy Related Laws (cont.)

- The ***Children's Online Privacy Protection Act of 1998 (COPPA)*** enacted on October 21, 1998
- This act, effective April 21, 2000, applies to online collection of personal information by persons or entities under U.S. jurisdiction from children under 13 years of age.
  - Requires a website operator to include in a privacy policy, when and how to seek verifiable consent from a parent or guardian, and what responsibilities an operator has to protect children's privacy and safety online, including restrictions on the marketing to those under 13.

*http://www.ftc.gov/opa/reporter/privacy/coppa.shtml

Export and Espionage Laws

- ***Economic Espionage Act of 1996 (EEA)***
  - Attempts to prevent ***trade secrets*** from being illegally shared
  - Designed to prevent abuse of information gained by an individual working in one company and employed by another

*http://en.wikipedia.org/wiki/Economic_Espionage_Act_of_1996

Export and Espionage Laws (cont.)

- ***Security and Freedom Through Encryption Act of 1999 (SAFE)***
  - Provides guidance on the ***use of encryption***
    - Clarifies *use of encryption* for people in the US
    - Permits all persons in the U.S. to buy or sell any *encryption product*
  - Provides measures of ***protection from government intervention***
    - Government cannot require use of any kind of key escrow system for encryption products.
  - Relax ***export restrictions*** by amending the Export Administration Act of 1979

* http://www.legalarchiver.org/safe.htm (1999)

Sarbanes–Oxley Act of 2002

- ***Sarbanes–Oxley Act of 2002***, ***Sarbox*** or ***SOX*** sets new or enhanced standards for all U.S. public company boards, management and public accounting firms.
  - As a result of SOX, top management must now ***individually certify the accuracy of financial information***. In addition, penalties for fraudulent financial activity are much more severe.
  - SOX increases the independence of outside auditors who review the accuracy of corporate financial statements, and increased the oversight role of boards of directors

Americans with Disabilities Act and Section 508 of Rehabilitation Act

- In 1998, Congress amended the Rehabilitation Act and strengthened provisions covering access to ***information*** in the federal sector, amended Section 508 covers ***access to all types of electronic and information technology in the federal sector and is not limited to assistive technologies used by people with disabilities***
- ***Americans with Disabilities Act of 1990***, is a wide-ranging civil rights law that ***prohibits, under certain circumstances, discrimination based on disability and is being increasingly interpreted to apply to the Internet***.
- In November, the National Federation of the Blind filed a landmark lawsuit against America Online (AOL). The suit claims AOL violated the federal Americans with Disabilities Act by failing to provide access for the disabled to its web based services.

U.S. Copyright Laws

- ***U.S. Copyright Law***
  - Copyright is a form of protection provided to the authors of "***original works of authorship***," including literary, dramatic, musical, artistic, and certain other intellectual works.
  - The copyright in the work of authorship immediately becomes the property of the author who created the work.
    - In the case of works ***made for hire***, the employer and not the employee is considered to be the author.
  - Copyright is secured automatically when the work is created, and a work is "created" when it is fixed in a copy or photorecord for the first time.
  - Complete 2010 version of the U.S. Copyright Law at *[***http://www.copyright.gov/title17/circ92.pdf***](http://www.copyright.gov/title17/circ92.pdf)

Freedom of Information Act

- ***Freedom of Information Act (FOIA)***
  - Allows any person to request access to federal agency ***records or information*** not determined to be a matter of ***national security***

  http://www.justice.gov/oip/foia_updates/Vol_XVII_4/page2.htm (1996)
- ***Electronic Freedom of Information Act amendments (E-FOIA)***
  - All government agencies must make "reading room" documents ***electronically available***

  http://www.balancedscorecard.org/EFOIA/tabid/113/Default.aspx (1996)

Jurisdiction and Authorities Related to Information Assurance

- **Jurisdiction** is the practical **authority** granted to a formally constituted legal body or to a political leader to deal with and make pronouncements on legal matters and, by implication, to administer justice within a defined area of responsibility
- In relation to information assurance, the jurisdictional authority would be responsible for maintaining entities' conformance to rules, laws and/or regulations set by government, organization or an individual.
- Several challenges regarding law enforcement due to the fact that laws are mostly geographically based, whereas data flow in an information system may not be geographically confined.

Payment Card Industry Data Security Standard (PCI DSS)

- ***PCI Security Standards Council*** offers robust and comprehensive standards and supporting materials to enhance payment card data security.
  - Including ***a framework of specifications, tools, measurements and support resources*** to help organizations ensure safe handling of cardholder information at every step.
- The keystone is **PCI Data Security Standard (PCI DSS)***, which provides a framework for developing a robust payment card data security process, including ***prevention, detection and reaction to security incidents***.

*https://www.pcisecuritystandards.org/security_standards/documents.php?document=pci_dss_v2-0#pci_dss_v2-0

Computer Ethics

- A set of ***moral principles*** that regulate the ***use of computers.***
- Some common issues include intellectual property rights (such as copyrighted electronic content), privacy concerns, and how computers affect society.
  - While it is easy to ***duplicate copyrighted electronic (or digital) content,*** computer ethics suggest that it is wrong to do so ***without the author's approval***.
  - While it may be possible to ***access someone's personal information on a computer system***, computer ethics advise that such an action is unethical.

Ten Commandments of Computer Ethics

- The **Ten Commandments of Computer Ethics** were created in 1992 by the Computer Ethics Institute to provide "a set of standards to guide and instruct people in the ethical use of computers."
- Widely quoted in computer ethics literature, but also have been criticized to be simplistic and overly restrictive.

*http://en.wikipedia.org/wiki/Ten_Commandments_of_Computer_Ethics

Ten Commandments of Computer Ethics (cont.)

- Thou shall not use a computer to harm other people.
- Thou shall not interfere with other people's computer work.
- Thou shall not snoop around in other people's files.
- Thou shall not use a computer to steal.
- Thou shall not use a computer to bear false witness.
- Thou shall not use or copy commercial software_for which you have not paid.
- Thou shall not use other people's computer resources without authorization.
- Thou shall not appropriate other people's intellectual output.
- Thou shall think about the social consequences of the program you write.
- Thou shall use a computer in ways that show consideration and respect....

References

- Michael E. Whitman, Herbert J. Mattord , *Principles of Information Security*, *4th Edition*, Course Technology, 2011
- Mark Stamp, *Information Security: Principles and Practice*, Wiley, 2011
- http://www.techterms.com/definition/computerethics