information technology & management

# business capabiliity SYSTEM INTEGRATION

ILLINOIS INSTITUTE OF TECHNOLOGY

ITMT430

## Law, Responsibility, & Professionalism

**Ray Trygstad**

ITMT 430 Spring 2017

2/16/17

# Objectives

At the conclusion of this lesson, students should be able to:

- Explain differences between law and ethics
- Recall the types of law in the U.S.
  - Define each type
- Explain the differences between statutory, regulatory and common law
- Recall and explain the structure of U.S. Federal Law

# Objectives

At the conclusion of this lesson, students should be able to:

- Discuss what standards of moral responsibility, legal liability, and accountability should apply in cases of information system malfunctions, especially in safety-critical systems
- Identify major national and international laws that relate to the employment of information technology

# Learning Objectives

Upon completion of this lesson, students should be able to:

- List applicable laws and policies related to employment of information technology
  - Describe major components of each pertaining to storage and transmission of data
  - Describe what the laws mandate and where they apply
  - List the applicable laws for compliance in a given situation

# Learning Objectives

Upon completion of this lesson, students should be able to:

- List applicable laws and policies related to employment of information technology
  - Describe how the type of legal dispute (civil, criminal, private) affects the evidence used to resolve it
  - Describe the impact of legal/regulatory standards on a given system

# Disclaimer

- I am not a lawyer, nor do I play one on television
- This lecture does not constitute legal advice, nor are there any guarantees or warrantees as the legal validity of any material included herein
- The aforesaid statements may or may not be enforceable depending on the jurisdiction, the day of the week, the wind…

# Ethics versus Law

- Law and ethics are not same thing
  - While many unethical things are illegal, many are not
  - An act can be unethical but perfectly legal
  - An action can also be perfectly ethical but illegal
    - U.S. businessman sentenced to eight years in U.S. prison for importing lobster tails in plastic bags instead of cardboard boxes in *possible* violation of Honduran law

http://www.overcriminalized.com/CaseStudy/McNab-Imprison-by-Foreign-Laws.aspx

# Difference Between Law and Ethics

- Laws - rules adopted and enforced by governments to codify expected behavior in modern society
  - Laws drawn from ethics
- Ethics define socially acceptable behaviors
  - Ethics based on cultural *mores*: the fixed moral attitudes or customs of a particular group

# Difference Between Law and Ethics

- Laws change over time
- Laws vary from state to state
- Political and economic interests, and not the interests of the people, often determine which laws get passed and what is in those laws
- Ethical standards transcend time, place, and the whims of politics



http://www.businessweek.com/stories/2007-10-15/if-its-legal-its-ethical-right-businessweek-business-news-stock-market-and-financial-advice

# Difference Between Law and Ethics

- Key difference between law and ethics is that law carries the sanction of a governing authority and ethics do not


http://www.irbsearchblog.com/wp-content/uploads/2014/04/blog-ethics-law.jpg

# Types of Law in the U.S.

- Criminal Law
  - Outlaw actions/activities that harm other people or property
  - Murder, larceny, rape, assault, DWI
  - Actively enforced through prosecution by the state

http://www.aegis-law.com/wp-content/uploads/2015/08/Criminal2.jpg

# Types of Law in the U.S.

- Civil Law
  - Disputes between people or groups, including disputes between governments and citizens
  - Contract disputes, divorce, child custody, property disputes, copyright laws
  - Violations are considered to be either torts or breaches of contract, rather than crimes

# Types of Law in the U.S.

- Constitutional Law
  - Violations of rights guaranteed by Constitution of the United States as well as some English Common Law
  - Person sues over excessive bail (8th amendment issue)
- Administrative Law
  - Cases involve law, rules and regulations that the U.S. executive branch and its agencies have implemented

# Types of Law in the U.S.

- International Law
  - Cases involving any law that affects the United States and any foreign nation, including laws that involve treaties, trade agreements, etc.
  - E.g. American fisherman not allowed to fish in waters in which trade agreements are met with another country

http://omidar.ir/wp-content/uploads/international-banner.jpg

# Types of Law

- Tort law
  - A civil wrong, *other than a breach of contract*, for which the law provides a remedy
  - Allows individuals to seek recourse against others in the event of personal, physical, or financial injury
  - Some torts are *criminal* (assault, battery), others are *civil* (libel, slander) while some can be either (trespass, negligence)

# Types of Law

- Tort law
  - Criminal torts differ from other criminal law as a case only exists if the wronged party pursues prosecution
    - i.e. files charges
  - Generally the state can only file charges without action of the wronged party if an agent of the state is a witness to the action
    - i.e. a police officer witnesses an assault

# Types of Law

- Private law
  - Civil law that regulates relationships between the individual and organizations other than government
  - Encompasses family law, commercial law, and labor law

# Types of Law

- Public law
  - Regulates structure & administration of government agencies and relationships with citizens, employees, and other governments
  - Includes criminal, civil, administrative, and constitutional law
  - Statutory law, based on statutes passed by legislative actions

# Types of Law

- *Regulatory* law
  - Law established by government agencies as directed by statutory law, to implement those laws through clarification and amplification of those laws
  - Written by bureaucrats and not by legislators

# Types of Law

- Case law
  - Law established by judicial decision in cases, often to clarify application of points of statutory, regulatory or common law
  - Sometimes establishes new law, which is part of *common law*

# Common Law

- Law established by judicial decisions, precedent, or commonly accepted usage rather than codified in statutes or regulations
- Pre-existing body of English common law generally has legal effect in the U.S. to the extent that legislation or the Constitution does not explicitly reject English common law

# English Common Law in the U.S.



- Establishes and implements many traditional legal rights such as easements, habeas corpus, jury trials, presumption of innocence, and various other civil liberties
- Generally "adopted" by state statutes or codified by specific statutes
- But not in effect in Louisiana…
  - …law based on the Code Napoleon

# Types of Law

- Proscriptive
  - "It is unlawful to…."
  - Against the law to do *something*
  - Most criminal law; criminal offenses are violations of proscriptive laws
- Prescriptive
  - "You must do the following…."
  - Against the law *not* to do *something*
  - Generally regulatory in nature

# Structure of U.S. Federal Law

- United States Code (U.S.C.)
  - Laws passed by the U.S. Congress & signed by the President – *statutory* law
  - In many (most?) cases direct executive branch to publish additional regulations
- Code of Federal Regulations (CFR)
  - Regulations published by executive departments and agencies as directed to implement laws in the U.S. Code
  - *Regulatory* law; has full force of law

# Responsibility, Liability, and Accountability

- Traditional models of responsibility require that two conditions be satisfied:
  - *causality*
  - *intent*
- For example, some agent, X, is held morally responsible for an act, Y, if X caused Y (or intended to cause Y)

# Responsibility

- A person could be held responsible for causing some outcome, even if he or she did not intend the outcome
  - For example, a person who carelessly left a campfire burning, which started a major forest fire, could be held responsible for causing the fire
    - Happened in 2014 with the Glendora fire in Los Angeles County in California

# Responsibility

- Agents can also be held responsible when they intend for something to happen, even if they ultimately fail to cause (or bring about) the intended outcome
  - For example, suppose a disgruntled student intends to blow up a computer lab, but is discovered at the last minute and prevented from doing so; even though the student failed to carry out his objective, we hold him morally culpable because of his intentions

# Liability vs. Responsibility

- *Liability* is a legal concept
- It is sometimes used in the narrow sense of "strict liability"
- To be strictly liable for harm is to be liable to compensate for it even though the party that is liable one did not necessarily bring it about through faulty action (e.g., when a someone is injured on a person's property)
- In liability incidents, the moral notion of "blame" may be left out

# The Legal Environment

- Information technology professionals/ managers must possess a rudimentary grasp of the legal framework within which their organizations operate
- Legal environments can influence the organization to a greater or lesser extent depending on the nature of the organization and the scale on which it operates

# Organizational Liability

- What if an organization does not support or even encourage strong ethical conduct on the part of its employees?
- What if an organization does not behave ethically?
  - If an employee, acting with or without authorization, performs an illegal or unethical act causing some degree of harm, organization can be held financially liable

# Organizational Liability

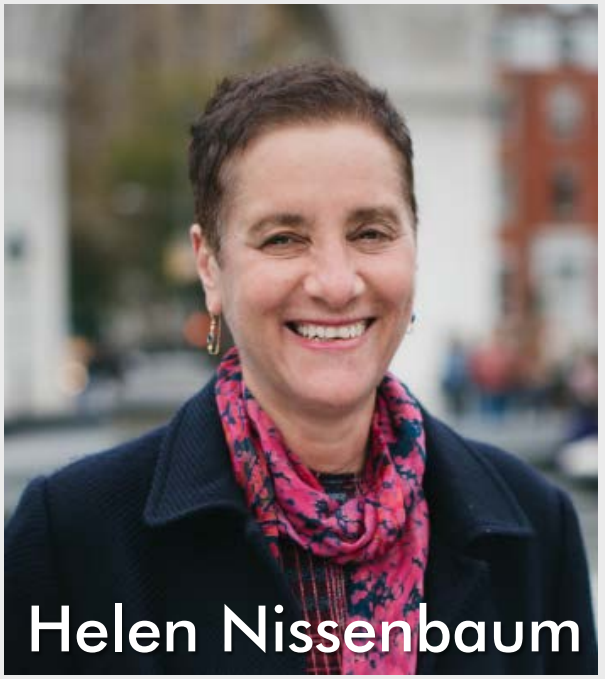
- ***Liability*** is the legal obligation of an entity
  - Liability extends beyond legal obligation or contract to include liability for a wrongful act and the legal obligation to make restitution
  - An organization increases its liability if it refuses to take strong measures known as ***due care***

# Organizational Liability

- ***Due diligence*** requires that an organization make a valid effort to protect others and continually maintain this level of effort
- Individual computing/IT professionals should always strive to use due care and exercise due diligence both personally and organizationally

# Accountability (vs. Liability and Responsibility)

- Helen Nissenbaum (2007) argues that responsibility is only part of what is covered by the (broader) notion of *accountability*
- For Nissenbaum, accountability means that someone, or some group of individuals, or even an entire organization is *answerable*


Helen Nissenbaum

# Accountability

- Nissenbaum points out that in cases of accountability,

  > ...there will be someone, or several people *to answer* not only for malfunctions in life-critical systems that cause or risk grave injuries and cause infrastructure and large monetary losses, but even for the malfunctions that cause individual losses of time, convenience, and contentment

# The Problem of "Many Hands" in a Computing Context

- Because computer systems are the products of engineering teams or of corporations, as opposed to the products of a single programmer working in isolation, "many hands" are involved in their development (Nissenbaum, 2007)
- It is difficult to determine who, exactly, is responsible whenever one of these computer or safety-critical system failures/accidents results in personal injury/harm to individuals

# Accountability vs. Responsibility

- *Accountability* is a broader concept than responsibility because it:
  a) is non-exclusionary
  b) can apply to groups, as well as to individuals

# Relevant U.S. Laws

- The U.S. has led the development and implementation of legislation to prevent misuse and exploitation of information and information technology
  - Promotes the general welfare and creates a stable environment for a solid economy

# Computer Fraud and Abuse Act of 1986

- A.k.a. the CFA Act
- Cornerstone of many computer-related federal laws and enforcement efforts
- Amended October 1996 by National Information Infrastructure Protection Act of 1996
  - Modified several sections of previous act
  - Increased penalties for select crimes

# Computer Fraud and Abuse Act of 1986

- Further modified by 2001 USA Patriot Act
  - Provides law enforcement with broader latitude to combat terrorism-related activities
  - USA Patriot = "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism"
- USA Patriot Act of 2001 was updated and extended, in many cases permanently, through the USA Patriot Improvement and Reauthorization Act of 2005

# Computer Security Act of 1987

- One of first attempts to protect federal computer systems by establishing minimum acceptable security practices
- Requires mandatory periodic training in computer security awareness and accepted computer security practice for all users of Federal computer systems
- Also established a Computer System Security and Privacy Advisory Board within the Department of Commerce

# Computer Security Act of 1987

- Assigned the National Bureau of Standards (now NIST) and the National Security Agency with development of:
  - Standards, guidelines, and associated methods and techniques for computer systems
  - Uniform standards & guidelines for most federal computer systems

# Computer Security Act of 1987

- Technical, management, physical, and administrative standards and guidelines for cost-effective security and privacy of sensitive information in federal computer systems
- Guidelines for operators of federal computer systems that contain sensitive information in training their employees in security awareness
- Validation procedures for, and evaluation of the effectiveness of, standards & guidelines through research and liaison with other government and private agencies

# Computer Security Act of 1987

- Amended Federal Property and Administrative Services Act of 1949, requiring NIST to distribute standards and guidelines pertaining to federal computer systems, making such standards compulsory and binding

# Federal Information Security Management Act of 2002

- Commonly known as FISMA
- Supersedes and updates Computer Security Act of 1987
- Mandates annual security audits of all federal computer systems

# Communication Act of 1934

- Provides penalties for misuse of telecommunications devices, specifically telephones
- Revised in 1996 by the Telecommunications Deregulation and Competition Act of 1996
  - Modified archaic language of the1934 Act
  - Title V was the Communications Decency Act

# Relevant U.S. Laws

- Communications Decency Act (CDA)
  - Immediately ensnared in a thorny legal debate over the attempt to define *indecency*, an area considerably broader than obscenity
  - Rejected by the Supreme Court

# Relevant U.S. Laws

- No Electronic Theft (NET) Act of 1997
  - Provides for criminal prosecution of individuals who, without authorization and *without realizing financial gain or commercial advantage*, electronically access copyrighted materials or *encourage others to do so* (inducement)
  - Prosecutions rare (only 8 in the first 5 years) and generally for egregious sharing of large numbers of files

# Relevant U.S. Laws

- No Electronic Theft (NET) Act of 1997
  - As best as I can determine, **no** prosecutions for "encouragement" or for peer-to-peer (P2P) file sharing
  - Government has been notably absent in charges/prosecutions of music file sharing as actively pursued in civil court by the Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA)

# Relevant U.S. Laws

- No Electronic Theft (NET) Act of 1997
  - In recent years, has led to seizure/ shutdown of websites by the FBI and DHS
  - One resulting criminal prosecution for "encouragement" (inducement) still pending against Kim Dotcom of Megaupload
    - Jurisdiction in the case is hazy—Megaupload is not a U.S. company
    - New Zealand has not extradited Kim Dotcom

# Relevant U.S. Laws

- Digital Millennium Copyright Act of 1998 (DMCA)
  - Intended to reduce the impact of copyright, trademark, and privacy infringement, especially through removal of technological copyright protection measures
  - More on this later

# Relevant U.S. Laws - General

- USA Patriot Act of 2001
  - Allows broader range of government and law enforcement action to combat terrorist activities
  - Many hold provisions & methods of enforcement of this act to be unconstitutional
    - Unconstitutional searches & seizures
    - "Secret" laws in CFR
    - Widespread warrantless collection of communications and digital information

# Relevant U.S. Laws - General

- Sarbanes-Oxley Act of 2002
  - Created to address accounting "irregularities" (Enron, etc.)
  - Requires internal controls & internal controls reporting which encompasses general computer controls which include information security
  - More on this later

# Relevant U.S. Laws - General

- Artist's Rights and Theft Prevention Act of 2005
  - Criminalizes taping of movies in theaters
  - Criminalizes making unreleased works intended for public distribution (beta version or workprints) available on a computer network accessible to members of the public

# Privacy Laws

- Many organizations collect, trade, and sell personal information as a commodity
  - Individuals are becoming aware of these practices and looking to governments to protect their privacy
- Aggregation of data from multiple sources permits unethical organizations to build databases with alarming quantities of personal information

# Privacy Laws

- Privacy of Customer Information Section of the section of regulations covering common carriers
  - Specifies that any proprietary information shall be used explicitly for providing services, and not for any marketing purposes

# Privacy in the U.S.

- Not a Constitutional right but has been construed by the courts
  - "Reasonable expectation" of privacy
- Working definition:
  - right not to be disturbed
  - right to be anonymous
  - right not to be monitored
  - right not to have one's identifying information exploited

# Privacy in the U.S.

- Construed Constitutional guarantees of privacy apply **only** to the Federal Government
- Privacy generally construed by interpretation of the Fourth Amendment of the U.S. Constitution, which prohibits search and seizure without a warrant

# Privacy Laws

- Federal Privacy Act of 1974 regulates the government's use of private information
  - Created to ensure that government agencies protect privacy of individuals' and businesses' information, and hold them responsible if this information is released without permission

# Privacy Laws

- Federal Privacy Act of 1974
- Exempt from some regulations so they can better perform their duties:
  - Bureau of the Census
  - National Archives & Records Administration
  - U.S. Congress (exempt themselves from most laws including Civil Rights Act and OSHA)
  - Comptroller General
  - Certain court orders
  - Credit agencies

# Privacy Laws

- Electronic Communications Privacy Act of 1986
  - Collection of statutes that regulates the interception of wire, electronic, and oral communications
- Both work in cooperation with the 4th Amendment of the U.S. Constitution
  - Prohibits search and seizure without a warrant

# Pivacy Laws: ECPA

- ECPA statutes address the following:
  - Interception and disclosure of wire, oral, and electronic communications
  - Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices
  - Confiscation of wire, oral, or electronic communication intercepting devices
  - Evidentiary use of intercepted wire or oral communications

# Pivacy Laws: ECPA

- ECPA statutes address the following:
  - Authorization for interception of wire, oral, or electronic communications
  - Authorization for disclosure and use of intercepted wire, oral, or electronic communications
  - Procedure for and reports concerning interception of wire, oral, or electronic communications
  - Injunction against illegal interception

# HIPAA

- Health Insurance Portability & Accountability Act Of 1996 (HIPAA), a.k.a. Kennedy-Kassebaum Act
- Protects confidentiality and security of health care data
  - Establishes and enforces standards
  - Standardizes electronic data interchange
  - Affects all health care organizations

# HIPAA

- Requires organizations that retain health care information to use information security mechanisms to protect this information, as well as policies and procedures to maintain them
- Requires comprehensive assessment of organization's information security systems, policies, and procedures

# HIPAA

- Privacy standards of HIPAA severely restrict dissemination and distribution of private health information without documented consent
  - Known as the HIPAA Privacy Rule
- Provides guidelines for use of electronic signatures
  - Based on security standards ensuring message integrity, user authentication, and nonrepudiation

# HIPAA

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

# ARRA and HITECH

- American Recovery & Reinvestment Act (ARRA) was designed to provide a response to the economic crisis in the U.S.
  - Included another act called the Health Information Technology for Economic and Clinical Health (HITECH)
- HIPAA and HITECH require that covered entities notify information owners of breaches

# Gramm-Leach-Bliley Act

- Financial Services Modernization Act or Gramm-Leach-Bliley Act of 1999
  - Applies to banks, securities firms, and insurance companies
  - Requires all financial institutions to:
    - Disclose privacy policies
    - Describe how they share nonpublic personal information
    - Describe how customers can request that their information not be shared with third parties

# Gramm-Leach-Bliley Act

- Financial Services Modernization Act or Gramm-Leach-Bliley Act of 1999
  - Ensures privacy policies are fully disclosed when a customer initiates a business relationship
  - Ensures privacy policies are distributed at least annually for the duration of the professional association

# Export and Espionage Laws

- Economic Espionage Act (EEA) of 1996
  - Attempt to protect intellectual property and competitive advantage
  - Attempts to protect trade secrets
    - "from the foreign government that uses its classic espionage apparatus to spy on a company, to the two American companies that are attempting to uncover each other's bid proposals, or to the disgruntled former employee who walks out of his former company with a computer diskette full of engineering schematics"

# Export and Espionage Laws

- Security and Freedom through Encryption Act of 1997
  - Provides guidance on use of encryption
  - Institutes measures of public protection from government intervention
  - Reinforces individual's right to use or sell encryption algorithms without concern for the impact of other regulations requiring some form of key registration
  - Prohibits federal government from requiring use of encryption for contracts, grants, and other official documents and correspondence

# Freedom of Information Act of 1966 (FOIA)

- Provides any person the right to request access to federal agency records or information, not determined to be in the interest of national security
  - US Government agencies required to disclose requested information on receipt of a written request

# Freedom of Information Act of 1966 (FOIA)

- Exceptions for information protected from disclosure
- Act does not apply to
  - Congress or Federal courts
  - state or local government agencies
  - private businesses or individuals
- Many states have their own version of the FOIA

# Freedom of Information Act of 2000 (UK)

- In 2000, the United Kingdom passed their Freedom of Information Act
  - Very similar in all respects to U.S. law
  - More exceptions

# Sarbanes-Oxley Act of 2002

- Enforces accountability for financial record keeping and reporting at publicly traded corporations
  - Requires CEO and chief financial officer (CFO) assume direct and personal accountability for completeness and accuracy of a publicly traded organization's financial reporting and record-keeping systems

# Sarbanes-Oxley Act of 2002

- As these executives attempt to ensure that the systems used to record and report are sound—often relying upon the expertise of CIOs and CISOs to do so—the related areas of availability and confidentiality are also emphasized

# What is a Copyright?

- Set of exclusive legal rights authors have over their works for a limited period of time; these rights include
  - copying the works (including parts of the works)
  - making derivative works
  - distributing the works
  - performing the works (showing a movie or playing an audio recording, as well as performing a dramatic work)

# What is a Copyright?

- Copyright exists **upon creation**
  - Author's rights begin when an original work of authorship is fixed in a tangible medium
  - Includes words published in electronic formats
- A work does not have to bear a copyright notice or be registered to be copyrighted

# US Copyright Law

- Intellectual property is recognized as a protected asset in the US
- US copyright law extends this right to the published word, including electronic formats
- Granted "for limited Times"…"To promote the Progress of Science and useful Arts" (Article I, Section 8, Clause 8, Constitution of the United States)

# US Copyright Law: Fair Use

- Fair use of copyrighted materials includes
  - the use to support news reporting, teaching, scholarship, and a number of other related permissions
  - the purpose of the use has to be for educational or library purposes, not for profit, and should not be excessive
- DMCA (more on this in a minute)

# What is Fair Use?

- Allow for limited copying or distribution of published works without author's permission
  - Examples:
    - Quotation of excerpts in a review or critique
    - copying of a small part of a work by a teacher or student to illustrate a lesson

# What is Fair Use?

- Determination of fair use based on:
  - Purpose and nature of the use
  - Nature of the copyrighted work
  - Nature and substantiality of the material used
  - Effect of use on the potential market for or value of the work

# What is Fair Use?

- Proper acknowledgement must be provided to author and/or copyright holder of such works, including a description of the location of source materials by using a recognized form of citation

# Licensing of Copyrights

- If fair use does not apply, using another's intellectual property requires a license
- A license is not a given—the owner does not have to grant a license nor give any explanation when they don't

# Licensing of Copyrights

- Placing materials on the Web does NOT place them in the Public Domain unless such assignment is specifically made
  - Some Web sites contain content such as clipart, buttons, bars, backgrounds, photos, where either the items have been placed in the public domain or a license for use is clearly granted
  - Otherwise all works online—graphic arts as well as text—are protected by copyright, and reuse requires a license

# Digital Millennium Copyright Act (DMCA)

- The Digital Millennium Copyright Act (DMCA) is the US version of an international effort to reduce the impact of copyright, trademark, and privacy infringement
- Many legal experts feel DMCA illegally infringes on Fair Use and has other adverse effects

# Impact of DMCA

- Critics claim DCMA has had the following impacts (among others):
  - DMCA is being used to silence researchers, computer scientists and critics
  - Corporations are using it against the public
  - Public/College radio stations can no longer afford to webcast

# Impact of DMCA

- Also has had a stifling effect on computer security research as prohibits the circumvention of copy protection and the distribution of devices that can be used to circumvent copyrights
  - In doing so it treats publishing of security vulnerabilities as a violation of the law

# SOPA (defeated!)

- Stop Online Piracy Act, H.R.3261
  - Far more draconian than DMCA
  - Would allow takedowns of entire sites based on accusations with no court action
  - Included felony penalties for noncommercial streaming infringement
  - Could have resulted in criminal prosecution of public libraries as well as complete shutdown of YouTube and most search engines

# Future of U.S. Info Security Laws

- Bills designed to protect consumers by requiring reasonable security policies and procedures to protect personal information:
  - Data Security Act of 2010
  - Data Security & Breach Notification Act of 2010
  - Cybersecurity Act of 2012
- All failed to pass
  - It is expected that similar legislation will inevitably make its way through Congress

# International Laws And Legal Bodies

- Many domestic laws and customs do not apply to international trade which is governed by international treaties and trade agreements
- Because of cultural differences and political complexities of the relationships among nations, there are few international laws relating to privacy and information security

# European Council Cyber-Crime Convention

- Empowers an international task force to oversee a range of Internet security functions and to standardize technology laws internationally
- Attempts to improve effectiveness of international investigations into breaches of technology law
- Overall goal: simplify acquisition of information for law enforcement agents in certain types of international crimes, as well as extradition

# European Union Model

- European Union Directive 95/46/EC effective October 1998 increases protection of individuals in processing of personal data & limits free movement of such data
  - Strong consumer protection
  - Only allows gathering of information necessary for transaction
  - Personal data cannot be transferred to another company without permission
- United Kingdom had implemented a version of this directive called the Database Right

# Australian High Tech Crime

- Australia's Computer Offences of the Criminal Code Act 1995 specifically includes:
  - Data system intrusions (such as hacking)
  - Unauthorized destruction or modification of data
  - Actions intended to deny service of computer systems to intended users such as denial-of-service (DoS) attacks
  - Creation and distribution of malicious software (a.k.a - malware)

# State & Local Regulations

- Each state or locality may have laws and regulations that impact the use of computer technology
- Information security professionals have a responsibility to understand state laws and regulations and insure organization's security policies and procedures comply

# Illinois Law

- Operating Internet gambling is criminal
  - "Knowingly establishes, maintains, or operates an Internet site that permits a person to play a game of chance or skill for money or other thing of value…"
  - (720 Illinois Compiled Statutes, Article 5/28-1(a)(12) )
  - (The wording would seem to make some fantasy football sites illegal…)

# Illinois Law

- *Illinois Computer Crime Prevention Law* makes **unauthorized computer use a criminal offense**
  - (720 *Illinois Compiled Statutes*, Article 5/16D)
  - Three offense categories are defined

# Illinois Computer Crime Prevention Law

- Computer Tampering
  - Access is gained to a computer, a program, or data, without permission from the owner
  - Unauthorized access: misdemeanor
  - Obtaining data or services: misdemeanor 1st offense; felony for subsequent offenses
  - Altering, damaging, destroying, or removing a computer, a program, or data: always a felony
  - Latter 2 offenses include use or attempted use of a "computer virus"

# Illinois Computer Crime Prevention Law

- Aggravated Computer Tampering
  - When computer tampering has the intended effect of
    a) disruption of or interference with vital services or operations of State or local government or a public utility, or
    b) creating a strong probability of death or great bodily harm to other individuals
  - Punishable as felonies

# Illinois Computer Crime Prevention Law

- Computer Fraud
  - When access to or use of a computer, program, or data is gained as part of a scheme to deceive or defraud
  - Includes use of a computer to gain control over money, services, or property

# Illinois Computer Crime Prevention Law

- Computer Fraud
  - In addition to its ordinary meaning, "property" in this context includes: electronic impulses, electronically produced data, confidential or copy-righted material, billing information, and software in any form
  - Punishable as felonies

# Defamation: Libel and Slander

- Generally civil injuries with enforcement by lawsuit
  - ***Slander***: malicious, false, & defamatory spoken statement
  - ***Libel***: malicious, false, & defamatory statement made through any other form of communication such as written words or images
  - Move is to treat statements that are offensive ***but*** are *true* or *opinion* as defamation (because way too many lawyers don't know the law very well…)

# Policy versus Law

- Key difference between policy and law:
  - Ignorance of policy is an acceptable defense
- Therefore policies must be:
  - Distributed to all individuals who are expected to comply with them
  - Readily available for employee reference
  - Easily understood, with multilingual, visually impaired and low-literacy translations
  - Acknowledged by employee with consent form
  - Uniformly enforced for all employees

# The End…

- Questions?