

# IT 4823

## Information Security Administration

### Legal and Ethical Considerations



Notice: This session is  
being recorded.

# Legal and Ethical Aspects

Today's topics include:

- Ethics and ethical issues
- Cybercrime and computer crime
- Intellectual property
- Privacy

# Introduction

- You must understand scope of your organization's legal and ethical responsibilities
- To minimize liabilities/reduce risks, the information security practitioner must:
  - Understand current legal environment
  - Stay current with laws and regulations
  - Watch for new issues that emerge

# Deterrence to Unethical and Illegal Behavior

- Deterrence: best method for preventing an illegal or unethical activity; *e.g.*, laws, policies, technical controls
- Laws and policies only deter if three conditions are present:
  - Fear of penalty
  - Probability of being caught
  - Probability of penalty being administered

# Ethics

“The study of the moral character of our rational, voluntary actions toward others.” –Sara Baase

Ethical behavior means “doing the right thing” with respect to our treatment of other people.

No simple rules.

# Liberties and Claim Rights

Two kinds of rights:

Liberties: impose no obligation, or at most an obligation to refrain from something, upon others.  
 (“negative” rights)

Claim rights: impose a positive obligation upon others.  
 (“positive” rights)

# No Simple Answers

*“In theory, there is no difference between theory and practice, but in practice there is.”*

— Jan L. A. van de Snepscheut

# Important Distinctions

Right, wrong and OK

Ethically obligatory

Ethically prohibited

Ethically acceptable

Distinctions between liberties and claim rights

Distinguishing wrong and harm

Separating goals from constraints



# Ethics and Personal Preferences

Is it ethical to answer your cell phone at dinner?

Is it rude?

Where is the line between personal preference and ethical behavior?

# Meyer's Rule of Ethics

*“In any ethical dilemma, the thing you least want to do is the correct choice.”*

—Meyer (From the Travis McGee novels)

Also Benedict Spinoza

# What is “Voluntary?”

“Ethics: The study of the moral character of our rational, voluntary actions toward others.”

Are your actions voluntary if they might cost you your job?

Does it depend upon how badly you need the job?

Why or why not?

# Professional Ethics

A professional claims certain expertise

Professionals have special responsibilities

To their customers

To the general public

# Professional Codes and Guidelines

Most professional organizations have codes of ethics or good practice

- Reminders of specific responsibilities
- Guidance for new members of the profession
- Handling of difficult ethical situations

# Rights as the Basis for Law

- What kinds of laws have their basis in liberties (negative rights) ?
- What kinds of laws that have their basis in claim rights (positive rights) ?

# Law and Ethics

“In a civilized society, law floats in a sea of ethics.”

– *Mr. Chief Justice Earl Warren*

# Law and Ethics in Information Security

- **Cultural mores:** fixed moral attitudes or customs of a particular group; systems of ethics are based on these.
- **Ethics:** define morally acceptable behavior.
- **Laws:** rules that mandate or prohibit certain societal behavior.
- Laws carry sanctions of a governing authority; ethics do not (but laws often have their basis in ethics)





# Types of Law

- **Criminal:** Violations are prosecuted by “the people,” with the possibility of imprisonment or even execution.
- **Civil:** Generally (but not always) two private parties. Monetary compensation without consideration of punishment or rehabilitation. Injunctions and restraining orders are possible
- **Tort:** A civil wrong other than breach of contract. Punitive damage awards are possible.

# Public and Private Law

- **Public law:** The law affecting relationships between individuals and the state.
  - Criminal law
  - Administrative law
- **Private law:** The body of law governing the relationships among individuals.
  - Contract law
  - Commercial law
  - Torts
  - Family law

# Organizational Liability

- Liability is legal obligation of an entity; includes legal obligation to make restitution for wrongs committed.
- An organization increases liability if it refuses to take measures known as due care or **due diligence**.
- Due diligence requires that an organization make valid effort to protect others and continually maintain that level of effort.

# Relevant U.S. Laws (General)

- Computer Fraud and Abuse Act of 1986 (CFA Act)
- Electronic Communications Privacy Act (ECPA)
- National Information Infrastructure Protection Act of 1996
- USA PATRIOT Act of 2001
- Telecommunications Deregulation and Competition Act of 1996
- Computer Security Act of 1987
- Digital Millennium Copyright Act (DMCA)
- Sarbanes-Oxley
- Gramm-Leach-Bliley
- HIPAA

# Export and Espionage Laws

- Economic Espionage Act of 1996 (EEA)
- Export controls on encryption and computing equipment.
- Export restrictions for encryption significantly relaxed, but still on the books.

# Key U.S. Federal Agencies

- Department of Homeland Security (DHS)
- Federal Bureau of Investigation's National Infrastructure Protection Center (NIPC)
- National Security Agency (NSA)
- U.S. Secret Service (Part of DHS)

# Policy Versus Law

- Organizations should develop and formalize a body of expectations called policy.
- Policies serve as organizational laws.
- To be enforceable, policy must be distributed, readily available, easily understood, and acknowledged by employees.

# Cybercrime / Computer Crime

- “Criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity”
- Categorized based on computer’s role:
  - as target
  - as storage device
  - as communications tool
- More comprehensive taxonomy seen in Cybercrime Convention, Computer Crime Surveys



# Special Laws for Computer Crime?

- If data are still there, how can copying be “theft?”
- As the textbook says, laws evolve. (Is a text message like email? Why or why not?)
- There are laws against unauthorized access or use.
- The DMCA (and other, less intrusive laws before it) address copying.
- Threats to confidentiality, integrity, and availability are now recognized as crimes.

# Computer Trespass

- “Unauthorized use of a computer,” *or* “use of a computer in excess of one’s authority.”
- In the U.S., various Federal and state laws
- A crime in many other countries.

# Problems with Prosecution

- Lack of understanding
- Lack of physical evidence
- Valuation of assets
- Complexity
- The issue of venue.

# Standards for Evidence

- Sufficient – convincing without question
- Competent – applicable according to law
- Relevant – material to the matter at hand

# Types of Evidence

- Direct: Oral testimony of personal knowledge
- Real: physical evidence
- Documentary: business records and the like
- Demonstrative: models, demonstrations, experiments

# Rules of Evidence

- Best evidence: original evidence is preferable to copies
- Exclusionary rule: evidence gathered illegally is not admissible.
- Hearsay rule: second-hand evidence is often not admissible. (See best evidence)
  - There are exceptions to the hearsay rule
  - Business records gathered *in the ordinary course of business* may be admissible

# "The Ordinary Course of Business"

- Log files
- Backups of email and other databases
- Monitoring records

The point is to collect continuously anything you are likely to need as evidence.

And *document* that you do so!

# The Chain of Evidence

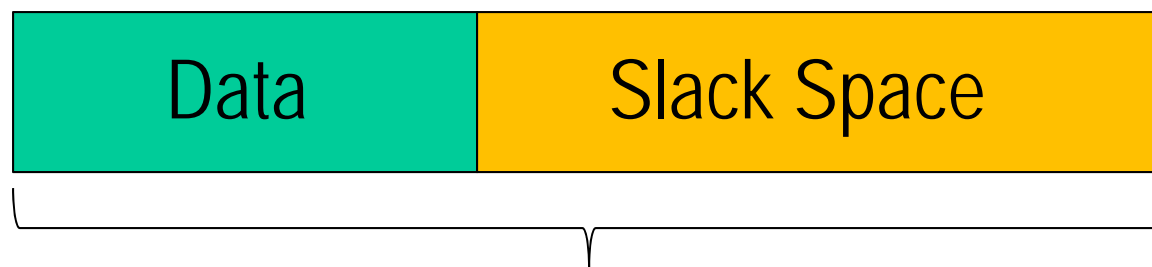
When evidence is collected other than in the ordinary course of business, it is important to provide proof that what is presented is what was found. This is the “chain of custody” and involves dated, signed, contemporaneous notes.

Message digests *may* be accepted as evidence that a file has not been changed since the digest was computed.



# Disk Drives

- Make an image copy (or two)
  - Gets free space
  - Gets file “slack space”
- Work with the image copy
- Preserve the original



One disk cluster (allocation unit)

## Get Help If...

- You are not *absolutely certain* you know what you're doing.
- You are dealing with evidence of a crime. (It is *also* a crime to tamper with or conceal evidence!)
- You are dealing with something that may become a civil legal matter.

# Sources of Help

- Your corporate counsel (or similar)
- Law enforcement
  - Take a detective to lunch
  - The time to get to know your local law enforcement people is *before* you need them
  - Consider carefully before involving law enforcement
- Forensics consultants (referrals from law firm or law enforcement official)

# Law Enforcement Involvement

- When an incident constitutes a violation of law, the organization may determine involving law enforcement is necessary
- Questions: (Decide these *in advance!*)
  - When should organization get law enforcement involved?
  - What level of law enforcement agency should be involved (local, state, federal)?
  - What happens when law enforcement agency is involved?

# Law Enforcement Involvement

- Some questions are best answered by organization's legal department or law firm.
- If organization detects a criminal act, it may be legally obligated to involve appropriate law enforcement officials
- It is helpful to have made contacts in advance, especially with local law enforcement.

# Advantages of Law Enforcement Involvement

Involving law enforcement has advantages:

- Agencies may be better equipped to process evidence
- Law enforcement agencies are prepared to handle warrants and subpoenas needed
- Law enforcement officers are skilled at obtaining witness statements and other information collection

# Disadvantages of Involvement

Involving law enforcement has disadvantages:

- Once a law enforcement agency takes over case, organization loses some control over chain of events
- Organization may not hear about case for weeks or months
- Equipment vital to the organization's business may be seized as evidence

# Encryption Law and Policy

1970's: Attempts to prohibit publication of research in cryptography.

1990's: Export restrictions; effect on competitiveness.

Now: An ongoing desire by law enforcement to read encrypted text; inference of crime by the presence of encryption. (More legislation proposed according to a September, 2010, story in the NYT.)



# “I Have Nothing to Hide!”

Some people will ask, “Why *shouldn't* the government have access to decryption keys? That will only bother people who have something to hide.”

# A Thought Experiment

A merchant uses strong encryption to protect the credit card numbers of his customers.

Does the merchant have “anything to hide” in the sense of the previous question?

# A Thought Experiment

A merchant uses strong encryption to protect the credit card numbers of his customers.

Does the merchant have “anything to hide” in the sense of the previous question?

- Can the merchant trust everyone who works for the government and might have access to decryption keys? (Reminder: the Georgia DMV employee.)
- Can the merchant be sure criminals cannot take control of the decryption system? (Reminder: the Italian phone tapping scandal.)

# Kinds of Property

- Real property, or real estate
  - Land
  - Buildings
- Personal property, or chattel
  - Car
  - Furniture
  - Clothing
- Intellectual property
  - Intangible, the result of the creative process
  - “Fixed” in tangible form

# Legal Protections

- Patents
- Trade secrets
- Trademarks
- Copyright

# Copyright Protection

- The U.S. Constitution gives Congress the power to provide for granting patents and copyrights.
- First copyright act in 1790
- Copyright is for a limited, but long, time. For authors, life plus 70 years; for corporate authorship, up to 120 years
- Copyright distinguishes between the tangible expression of a work and the creative part.

# Requirements for Copyright

- A work must be “creative.”
- It must be “fixed” in a tangible medium.
- Any creative work can be protected. Examples:
  - Books
  - Photographs
  - Poetry
  - Computer programs!
- In the U.S., copyright protection exists as soon as a creative work is “fixed.”
- A notice is still a good idea!

# Aspects of Privacy

- Freedom from intrusion. (The right to be let alone.)
- Ability to control information about oneself.
- Freedom from surveillance (*i.e.* from being tracked, watched, eavesdropped upon.)



# Is Privacy a Good Thing?

- *Is privacy a good thing?*
- What is “personal information,” anyway?
- Why are we interested in preserving privacy?

# Privacy Threats

- Intentional uses
  - Law enforcement
  - Tax collection
  - Marketing!
- Unauthorized use
- Theft
- Leakage of information
- Our own actions

# Risks

- Search queries
  - DoJ subpoena in COPA case
  - AOL release
- Can individual be identified through search queries?
- Anything we do on line is recorded
- Everything that is recorded is saved forever.

# Invisible Information Gathering

- Facebook and Twitter and Google – Oh, my!
- That cartoon cursor
- ISP logs
- Event data recorders in cars
- RFID tags
- Web cookies
- Programs that phone home
- Supermarket and other discount cards

# Secondary Uses

- Any use other than that for which the information was gathered
  - Example: find deadbeat dads through tax returns
- Data mining: Connecting multiple databases through a common identifier, such as SSN.
- Profiling, *e.g.* to detect fraud.

# Privacy Principles

- Informed consent
- Collection of only the data that is needed
- Provide for opting out
- Provide extra protection for sensitive data
- Destroy data after it is no longer needed
- Maintain accuracy of data
- Keep data secure
- Maintain policies for responding to law enforcement requests

# Fighting Terrorism

- Are names (alone) a reliable way to match records or identify people?
- What about names in other languages? Originally written in other alphabets?
- That terrorist “special screening” list...
  - Some “Bob Brown”
  - An eight year old boy
  - A retired military officer
  - A nun
  - An airline pilot!

# Other Government Databases

- Tax records
- Medical records
- Marriage and divorce records
- Property ownership
- Welfare
- School records
- Motor vehicle registration
- Many others...



# Privacy Act of 1974

- Only “relevant and necessary” data
- Notice of record systems
- Right of access
- Security
- Prohibition against disclosure (with exceptions)

*Should the government buy data it is not allowed to collect?*

# Tracking College Students

- We spend billions of dollars on grants, loans, and direct subsidies.
- Shouldn't we verify that we are getting value for this tax money?
- So... we need a database of every college student and how they are performing, right?

## *Quis custodiet ipsos custodes?*

*Who will guard the guardians?*

- Uses of census data:
  - World War I draft
  - World War II interment of Japanese Americans.
- The FBI's CODIS DNA database
  - Originally, convicted sex offenders
  - Then murderers were added
  - Some states require DNA if convicted of a misdemeanor.
  - Some states collect DNA from people arrested (but not yet convicted)

# The Social Security Number

Social Security Number as ID number

Matching

Access to information

Identity theft

The SSN as a national ID number?

# National ID Cards

Benefits of a national ID card

- fewer cards to carry(?)

- harder to forge

- deter identity theft

And the down side?

- “Your papers, please!”

- Do you need an ID to work?

What about the “Real ID” law? (Passed in 2005; implementation in 2008 – 09.)

# Health Information

- Medical databases are replacing paper records
- Are databases easier or harder to protect?
- What are the legitimate uses of medical records?
- Medical records and payment for health care.
- Medical records and sensitive conditions.
- Risks of health insurance fraud.

# Laws about Medical Privacy

HIPAA: Health Insurance Portability and Accountability Act (Administrative Simplifications)

Privacy protections  
Security requirements

And also... standardization of identifying codes,  
and ...government access without a consent  
requirement

# Public Records

- Property ownership records
- Marriage licenses
- Bankruptcy records
- Criminal records

What is the effect of computers?

Aircraft flight plans

Judges' financial disclosures



# The Fourth Amendment

*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated...*

# The Fourth Amendment

- The Fourth Amendment and the expectation of privacy...
  - Katz v. United States (phone taps)
  - Kyllo v. United States (thermal imaging)
- Non-invasive searches
  - Thermal imaging
  - Backscatter X-Ray
  - Drug-sniffing dogs
  - Telephone records (and the Third Party doctrine)

# The USA PATRIOT Act

- Many kinds of records available without court oversight.
- National Security Letters – Compel production of information without a warrant
  - Intended for emergencies
  - Widely misused by the FBI

# Questions

