Computer Forensic
Evidence Collection and Management

Chapter 2

Policies, Standards, Laws, and Legal Processes

Chapter Objectives

- Look at the numerous laws and statutes that apply to computer-related crimes
- Become familiar with acceptable electronic evidence
- Identify various techniques employed in court proceedings
- Determine expert witness requirements
- Look at sample security and computer-use policies and standards
- Differentiate between security policy violations and criminal activities
- Become familiar with numerous definitions of legal terms.

Introduction

- A computer crime involves the use of high tech equipment to facilitate conventional crimes and permeates every aspect of society including the work place
- Computer and electronic devices can be vehicles for committing various crimes; they may contain valuable evidence.
- A computer forensics specialist or subject matter expert is extremely valuable to assist in all stages of building a case.
- Evidence recovered in these situations is easily compromised and can therefore be ruled as inadmissible I court proceedings.

Laws and legal Issues

- Law can be categorized:

Civil Law:
Represents numerous laws recorded in volumes of legal code

Criminal Law:
Addresses violations enforced through state prosecution

Tort Law:
Allows individuals to seek redress in the courts

There are a variety of legal issues facing the computer-crime specialist. Understanding these issues is critical to the effective prosecution of criminals.

Several important laws and various issues that must be addressed include:

- *Electronic Communications Privacy Act (ECPA)*
- *Cable Communications Privacy Act (CCPA)*
- *Privacy Protection Act (PPA)*
- *USA Patriot Act of 2001*
- *Search and seizure requirements of the Fourth Amendment*
- *Legal right to search the computer media*
- *Legal right to remove the computer media from the scene*
- *Availability of privileged material on the computer media for examination.*

Electronic Communications Privacy Act

ECPA states that people have a reasonable expectation of privacy in their telephone use. Two parts of the ECPA address wiretaps and stored electronic communications:

Wiretaps:

- Wiretapping is the monitoring of telephone conversation by a third party, often by covert means. It is a felony to intercept any of the three types of protected communications absent a statutory exceptions. Example of wiretapping include keystroking, sniffing, and cloned e-mail. Wiretapping exceptions include a court order for intercept, consent, and provide protection exception., and inadvertently obtained information.

Stored Electronic Communications:

- It refers to e-mail while it resides on an e-mail server. This doesn't not apply to e-mail that resides on an end user's computer. There are two categories of stored electronic communications: an electronic service provide which provides users with the ability to send or receive wire or electronic communications. Example includes AOL; and a remote computer service, which utilizes a system that provides computer storage or processing services to the general public. Example includes an Internet Service Provider.

It is a misdemeanor for an electronic communications service or remote computing service to voluntarily disclose content of electronic or wire communications absent a statutory exception.

Privacy Protection Act

- It was designed to protect people involved in first amendment activities from searches when they themselves are not involved in criminal activity. It primarily protects work product and documentary materials.
- Exceptions include: Probable cause that the person possessing material has committed or is committing a criminal offense. Items are contraband or fruits of a crime and immediate seizure is needed to prevent death or serious bodily injury to a human being. There is reason to believe that notice would result in the destruction of material.
- This act only applies to search warrants and court orders.

Cable Communications Privacy Act

- It prevents a cable company from releasing personally identifiable information about a subscriber unless the government offers clear and convincing evidence that the subscriber is a suspect and the subscriber is given an opportunity to contest the issue at an adversarial hearing.
- Data collection is limited to that which the system regards as necessary to maintain daily operations, such as billing records, maintenance and repair orders, premium service subscription and subscriber complains.

USA Patriot Act

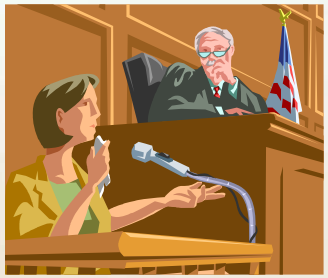
- It was a response to the 9/11 attacks. It amends portions of both ECPA and CCPA. The act deters and punishes terrorist activates in the United States and around the world, and enhances law enforcement investigation tools.
- It expands federals agencies' power in intercepting, sharing and using private telecommunications, especially electronic communications, focusing on criminal investigations by updating the rules that govern computer-crime investigations.

The fourth Amendment

- The Fourth Amendment can be broken down into two distinct parts.
  - The first part provides protection against unreasonable searches and seizures
  - The second part of the amendment provides for the proper issue of warrants.
- There are Fourth Amendment implications for searching and retrieving data from computer and electronic devices. Theses include the legal right to search the computer media and to remove it from the scene.

Witness

- A witness is described as someone who testifies to what he or she has seen , heard or otherwise observed and who is not a party to the action.
- A subpoena is a process to cause a witness to appear and give testimony, commanding and appearance before a court therein named at a time therein mentioned to testify for the party named under a penalty therein mentioned.
- No person has to provide information that is self-incriminating, either as a witness in a trial or in response to police questioning.
- An evidence obtained by unlawful search or seizure by police is inadmissible in court; it is considered more important to maintain legal protection for all than to convict guilty parties.



- *Indirect testimony* is evidence providing only a basis for inference about the fact in dispute.
- *Direct testimony* includes statements made under oath by a party or the party's witness.

Evidence

- Evidence provides the means by which disputed facts are proved to be true or untrue in any trial before a court of law or an agency that functions like a court.
- Evidence must be produced on given points by one side or the other in a court trial.
- Rules of admissibility determine which items of evidence judge or juries may be permitted to hear, see or read.
- Hearsay evidence consists of statements made out of court by someone how is not present to testify under oath at a trial.
- Legal evidence is not limited to the sworn testimony of witnesses.
- The evidence presented by the prosecution of by the defense may consist of the oral testimony or witnesses, documentary evidence and physical evidence, such as a cell phone or a mouse with the defendant's fingerprints on it.

Search Warrants

- A search warrant, in criminal law, is an order of a court, usually of a magistrate, issued to an officer of the law. This order authorizes a search of the premises named in the warrant for stolen articles, property possessed in violation of the law, or the instruments or evidence of a crime.
- Under the Fourth Amendment a search warrant can be issued only on oath of a complainant showing probable cause for its issuance.

Discovery

- Modern civil litigation is based upon the idea that the parties should not be subject to surprises at trial.
- *Discovery* is the process whereby civil litigants seek to obtain information from other parties and from nonparties or third parties. Parties can obtain information with a series of tools:
  - *Document request:* A party can seek documents and other real objects from parties and non parties
  - *Interrogatories:* A party can require other parties to answer questions
  - *Request for admissions:* A party can require other parties to admit or deny the truth of certain statements.
  - *Depositions*: A party can require individuals or representatives of organization to make themselves available for questioning.

Electronic discovery (E-discovery) refers to any process in which electronic data is sought, located, secured, and searched with the intent of using is as evidence in a civil or criminal legal case.

Interrogatives and Request for Production

- Request for interrogatories and production of documents must be in accordance with applicable civil and local rules of the court where the matter is filed.
- There are number of terms and definitions that apply in the interrogatory and production process:
  - Application software
  - Archive
  - Backup
  - Computer
  - Data
  - Digital Camera
  - Document
  - Hard drive
  - Help features/documentation
  - Imaged copy
  - Input device
  - Magnetic or optical storage media
  - Network
  - OS
  - Network OS
  - Software
  - Storage devices
  - Storage media

- There are several request that might be required pertaining to the preservation of evidence. These include:
  - Written policies on preservation of records
  - Destruction of documents
  - Person in charge of maintaining document retention and destruction policies
  - Preservation of evidence
  - Storage of documents.

Hacking involves advanced computer skills for breaking into computers and networks.

Law Relating to Compute Crimes

- Security is defined as freedom from risk or danger, and freedom from doubt, anxiety, or fear.
- Privacy is defined as being secluded from the sight, presence, or intrusion of others.
- Individuals and organization must be aware of various laws that have been enacted to protect the privacy of electronic data.

Heath Insurance Portability and Accountability Act

It was enacted by the US Congress in 1996. It requires the Department of Health and Human Services to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers. It also addresses the security and privacy of health data.

Sarbanes-Oxley Act

On July 30, 2002, the Sarbanes-Oxley (Sarbox) Act went into effect. The law establishes stringent financial reporting requirements for companies doing business in the United States. It defines the type of records that must be recorded and for how long. It also deals with basification of data.

Children's Online Privacy Protection Act of 1998

It is effective on April 21, 2000. It applies to the online collection of personal information by persons or entities under US jurisdiction from children under age 13. It spells out what a Web site operator must include in a privacy policy, when and how to seek verifiable consent from a parent and what responsibilities an operator has to protect children's' privacy and safety online.

Law Relating to Compute Crimes (cont.)

The Computer Security Act

The computer Security Act of 1987 provides for improving the security and privacy of sensitive information in federal computer systems. The security measures in any system are what enable it to operate fully, including maintaining privacy.

The Privacy Act of 1974

The purpose of the Privacy Act is to balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from federal agencies' collection, maintenance, use, and disclosure of personal information about them.

Uniform Electronic Transactions Act (UETA)

It provides a legal framework for electronic transactions. It gives electronic signatures and record the same validly and enforceability as manual signature and paper-based transactions.

Electronic Signatures in Global and national Commerce Act

It establishes the validity of electronic records and signatures. It governs in the absence of a state law or where states have made modifications to UETA that are inconsistent with the E-SIGN.

Uniform Computer Information Transaction Act

It will impact the music industry, the information technology industry, public and private libraries, data processing service providers, publishers of statistical data, traditional print publishers, online database providers, and the consumer of information.

E-Mail Laws

There are several laws that apply specifically to electronic mail. There are different rules for these situations:

Title 18 USC Section 2511 – Interception of Communication (Interception in Transit)
No person may intentionally intercept or attempt to intercept, or authorize or procure any other person to intercept or attempt to intercept , at any place in the Republic, any communication in the course of its occurrence or transmission.

Title 18 USC Section 2701-2711-Electronic Communications Privacy Act (ECPA) (Unlawful Access to Stored Communications)
ECA prohibits unlawful access and certain disclosure of communication contents. Additionally, the law prevents government entities form requiring disclosure of electronic communications from a provider without proper procedure.

Computer Crime and Intellectual Property Section (CCIPS)

This provides information on two categories of laws that are relevant to both security and law-enforcement organizations. Cases can be thrown out due to improper procedures undertaken during the various stages of a forensic investigation. Relevant laws include:

- ❑18 USC & 1362 – Communication Lines, Stations, or Systems
- ❑18 USC & 2510 – Wire and Electronic Communications Interception and Interception of Oral Communications
- ❑18 USC & 2710 – Stored Wire and Electronic Communications and Transactional Records Access
- ❑18 USC & 3121 – Recording of Dialing, Routing, Addressing, and Signaling Information

Policies and Standards

The Federal Accounting Standards Advisory Board (FASAB) is the body that establishes accounting principles for federal entities.

Generally Accepted Accounting Principles (GAAP)

These are the accounting rules used to prepare financial statements for publicly traded companies and many private companies in the United States.

ISO 17799 code of Practice for Security Management

It provides best practice recommendations on information security management for use by those who are responsible for initiating, implementing or maintaining information security management systems.

Information Technology Evidence Standards

This includes:

- ❑Guidelines for evidence collection and archiving
- ❑Guidelines for best practice in the forensic examination of digital technology
- ❑Best practices for computer forensic.

Policies

Organizations can avoid litigation and unnecessary grief by publishing and maintaining policies that employees and other interested parties find easy to read and observe. These policies would set forth the rules concerning the use of the organizations' computer, electronic, and network resources.

Computer resource policies

Policy statement are usually approved by an organizations' officers and legal staff.

Computer-Use Requirements and Restriction

Acceptable computer-use policies are usually specific to the organization. Computer–use policies are usually established by IT management.

Organizational Security Policies

A security policy is a generic document that outlines rules for computer network access, determines how policies are enforced, and sets forth the basic architecture of the organization's security environment.
A security architecture is a detailed description of all aspects of the system that relate to security, along with a set of principles to guide the design. The architecture includes the following:

- Security audit
- Security countermeasures
- Security features
- Security perimeter
- Security requirements

Audits and investigation might be directed at a security violation or a security incident.

Internal Investigation

Before security resources are allocated to investigating some internal complaint or incident, a determination must be made as to the credibility of the complaint. There may be political and adverse organizational consequences, including significant costs of conducting an overt investigation.

Civil and Criminal Computer Incidents

Many computer users, including juveniles and students, will try anything to see if they can do it. Thee individuals are often called “script kiddies”. Examples of such acts include but are not limited to excessive game playing, sniffing, spamming, Initiate denial-of- service (DoS) attack.

Security Departments

Many large corporations, governments offices, and educational entities have an internal department that is charged with protecting the organization’s capital resources. These functions include the protection of physical facilities, various assts, and information system and technology resources.

Civil Litigations

Civil litigations begins when plaintiff request access to a computer hard drive, via a court order or agreement. Generally the forensic expert makes a forensic copy of the drive for analysis. Often the defendant is required to provide the drive for a lengthy time period. The plaintiff requests the forensic expert to identify, locate, and isolate specific information contained on the hard drive.

Criminal Prosecution

Currently criminal procedure puts the burden of proof on the prosecution. It is p to the prosecution to prove that the defendant is guilty, as opposed to having the defendant prove any innocence; thus any doubt is resolved in favor of the defendant.

Law Enforcement Involvement

The following is a list of government offices and watch dog groups that address various aspects of computer forensics and to other law enforcement initiatives.

- FBI: A federal law enforcement agency that investigates alleged violations of federal criminal laws governing banking, gambling, white collar fraud, public corruption, etc.
- SEARCH: Provides the tools for justice system organization to work together to solve communication problems and to implement standard practice.
- HTCIA: Designated to encourage, promote, aid and affect the voluntary interchange of data, information, experience, ideas and knowledge about methods, processes, and techniques relating to investigations and security in advanced technologies among its membership.
- FACT: A not-for-profit association for the purpose of training law enforcement in the scientific techniques of examining computers.
- NWC3: Provides a nationwide support system for agencies involved in the prevention, investigation, and prosecution of economic and high-tech crimes.
- USPIS: Its mission is to protect he US Postal Service , its employees and its customers from criminal attack, and protect the nation’s mail system from criminal misuse.

Expert Witness and Computer Forensic Experts

•Evidence resulting from a computer forensic investigation can mean the difference between wining and losing a case.
•Computer forensics specialist and examiners are trained in specific techniques applicable to the field.
•Experts in other compute related fields are not generally trained in forensics.
•A new category of subject matter expert is the forensic account which is trained in the fundamentals of accounting and financial management and uses computer technology resources to identify questionable or illegal financial activates.
•The earlier a forensic specialist, forensics investigator, or forensics examiner is involved in the matter, the greater the chance that usable evidence will result from the investigation

•A computer forensics specialist or subject matter expert (SME) will be extremely valuable to assist in all stages of building a case, including:

- ❑Ascertaining whether the device(s) may contain information relevant to the subject of concern.
- ❑Assisting in preparing and responding to interrogatories (written question)
- ❑Planning and providing expert testimony
- ❑Retrieving and examining information that is accessible only through the use of forensics techniques, software, hardware and methods
- ❑Developing court reports.

•The National Institute of Justice has developed methods for electronic investigations and forensic analysis.