Police and Technology: Investigations and Legal Issues

Lecture Outline

1. Law Enforcement Response: Federal
2. Law Enforcement Response: State & Local
3. Investigations
4. Single Crime Scenes
5. Multiple Location and Network Crime Scenes
6. Jurisdiction Issues

Federal Agencies and Cybercrime

While cybercrime issues are decidedly national and international in their scope, the response to these crimes has been handled mostly from the National level.

Although many states and some large local jurisdictions have established good cybercrime units, law enforcement response is largely at the federal level for cybercrimes.

**Importantly, this is largely because they have the technical expertise AND political clout to obtain the financial and operational resources necessary.

This federal response has been fairly recent in nature and has resulted in the creation of new units and the hiring of technically skilled officers like never before.

Secret Service

Created in 1865, this agency is one of the oldest Federal law enforcement agencies, and one of the lead agencies in cybercrime issues.

While they are best known for their work on counterfeiting and protective services, they are also the primary federal agency on computer and cybercrime issues.

Majority of the computer/cyber crime is handled through the Financial Crimes Division

The main cybercrime areas they deal with are:

* Financial Institution Fraud

* Device Fraud

* General Computer Fraud relating to computers and systems of “Federal Interest”

Secret Service

Financial Institution Fraud:

USSS has concurrent jurisdiction with the DOJ to investigate fraud committed against financial institutions such as Banks and savings & loans.

Mostly this is counterfeiting, but increasingly it involves fraud relating to computers and spam

Fake e-mails sent to and from Banks.

Device Fraud:

Involves credit card fraud as well as PIN numbers, and passwords.

Increasingly investigating computer code theft relating to cellphones and the tracking of billing information.

Secret Service

General Computer Fraud:

Involves computers and systems with a “federal interest”

This section includes computers, not only as an instrument of the crime, but to "hack" into data bases to retrieve account information; store account information; clone microchips for cellular telephones; and scan corporate checks, bonds and negotiable instruments, that are later counterfeited using desktop publishing methods.

Because computers are a tremendous source of both investigative leads and evidentiary material, the Secret Service has established the Electronic Crimes Special Agent Program (ECSAP)

ECSAP trains agents to conduct forensic examinations of computers that were used in criminal endeavors. So trained, these agents can preserve any investigative leads within the computer, as well as any evidence needed for subsequent prosecutions.

Electronic Crimes Branch

Department of Justice

The DOJ is a vast array of sections and subunits designed to oversee the administration of justice at the federal level.

Agencies under the DOJ include:

* U.S. Attorney's offices: Prosecution

* Investigative Agencies: FBI, DEA, ATF, ICE

* Immigration and Naturalization

* US Marshals

* Bureau of Prisons

Main area within the DOJ for dealing with Cybercrime is the Computer Crime and Intellectual Property Section (CCIPS) within the Criminal Division.

Department of Justice

This unit Primarily prosecutes violations of Federal Code covered by Title 18 Section 1030 of the Computer Fraud and Abuse Act.

Currently the section employs only around 32 attorneys who focus solely on legal issues raised by computer and intellectual property crimes

Specifically, they focus on prosecuting crimes related to encryption, e-commerce, IP, Privacy laws, Hacker investigations, and search an seizures of computers.

Also advise on legality of pending computer crime legislation

Starting to provide training as there is a growing interest in this area and few outlets for training by accomplished people.

DOJ is also expanding its CHIP (Computer Hacking and Intellectual Property) Unit to assist in investigation.

**Little of what is done by the DOJ actually involves investigation, majority of the money is funneled toward prosecution.

Federal Bureau of Investigation

The largest of the Federal investigation agencies focuses on cybercrime issues in two main ways.

1. Investigates domestic criminal acts involving computers.
2. Collaborates with other agencies to protect Critical Infrastructure.

In addition the FBI has 3 computer forensic laboratories nationwide which provide tremendous support to local and state agencies.

The FBI has also recently developed the CAT teams, that are small teams that travel around the world to assist in cybercrime investigations.

In addition, the FBI works with other groups on infrastructure protection and White Collar Crime reporting related to technology.

Federal Trade Commission

This agency was largely created in order to deal with anti-trust issues of the 1920’s, but has evolved into a technology driven agency.

While they are largely and anti-trust agency, they also focus on protecting consumer markets and through this they get involved in cybercrime.

* False marketing claims

* Credit Card scams

* Financial Pyramid Schemes

* Fraudulent business opportunity schemes

The FTC is also one of the main groups involved with preventing Identity Theft at the federal level.

Largely the FTC provides assistance to state and local agencies on Identity Theft issues rather than investigate the crimes themselves.

U.S. Postal Service

The Postal Inspection Service is one of the oldest Federal Law Enforcement agencies in existence.

Been in existence since 1830

The Postal Inspectors are involved mostly in cybercrime through assisting in joint investigations with other federal agencies.

The main crimes they are involved in are:

- **Identity Theft**: Usually involved because of stolen mail.
- **Child Exploitation and Pornography**: The lead agency in the fight against Child Porn in the U.S.

  They take the lead in these types of investigations

  Increasingly, child porn is a cyber only crime.
- **Electronic Crimes**: Postal Inspectors share jurisdiction with agencies when any electronic crime involves the misuse of the mail

State and Local Roles in Cybercrime

While the federal system has appeared to jump on the cybercrime issue over the last 10-15 years, state and local agencies are still just starting to realize the nature of the issue.

Reasons for the late recognition of Cybercrime

1. **Number of Agencies**: Approximately 16,500 state and local agencies, causing confusion about who should do what.
2. **Funding**: Most local agencies are small and underfunded.

In combination, poor, small, and fractured agencies do not handle high-tech crimes well.

**Importantly, despite these poor conditions for investigations and enforcement, surveys of local law enforcement report an increased reporting of computer related crimes.

In particular, fraud and theft using computers reports have increased among local and state agencies.

Child porn and other exploitation crimes are also increasing.

State and Local Roles in Cybercrime

Recent research into computer related crimes and their handling on the state and local level has found that several areas are of critical importance to improving state and local response.

In particular 4 critical needs have been identified

1. **Training**: The vast majority of local agencies receive very little training at all much less technology related training.

Lack of training leads to patrol officers destroying evidence, not recognizing crimes, and ignoring citizen complaints.

2. **Equipment Needs**: Most local agencies have woefully inadequate equipment in terms of computers and technology.

When S.E. KY was given a grant to upgrade technology for 110 agencies the first thing they had to do was give all agencies Fax machines, phones, and A computer.

Those agencies that have computers often have outdated equipment.

Many agencies rely on individual officers to provide their own equipment.

State and Local Roles in Cybercrime

3. **Updated Criminal Codes**: Criminal codes need to be updated to complement current enforcement efforts.

Statutes are often years behind technology in terms making enforcement realistic.

Example: Enforcement of subpoenas across state lines is not currently possible despite a real need with computer crimes.

How do you investigate an internet related crime without the ability to subpoena individuals who live elsewhere.

4. **Collaboration**: It is exceedingly difficult for local agencies to work with experts at the federal level or to work with other local agencies.

Despite there is great levels of expertise at the federal level, it is difficult for local agencies to find these resources.

There is no central contact point or list of contact points.

Moreover, local agencies do not even have a list of all services available to them.

Investigations

This section of the lecture will cover several different areas:

1. Investigator roles and responsibilities.
2. Guidelines for handling searches and seizures.

While this class is not designed to teach you investigation skills, this section is designed to show you the technological sophistication required to deal with cybercrime and computer crime issues.

Importantly, it will help you understand the major problems that local police agencies face when dealing with these types of crimes in their jurisdictions.

Investigator Roles and Responsibilities

Although only the largest of all local police agencies have the funds and the needs to establish a full time electronic crime investigation unit, many agencies are experiencing computer crimes.

As discussed earlier, most local agencies do not have much sophistication when it comes to dealing with computer crimes.

Generally, the role and responsibility of police staff in computer crimes is the same as it would be in a normal crime, with the exception of a few unique issues.

- First Responders
- Investigators
- Forensic Analysts

First Responders

First responders are most often patrol officers who have little training in investigations or evidence collection.

Most of the time first responders are trained to leave everything alone and try and preserve the crime scene in its original setting.

Duties of First responders:

- Tending to injured
- Isolating suspects
- Controlling onlookers
- Preserve evidence

Electronic evidence has been largely overlooked in training and because of this, critical evidence is often mishandled and contaminated.

Types of Electronic Evidence

* Cellphones, PDA's, Computers, Smartcards, CD's, DVD's, Flash drives, Hard drives, Cameras, Watches, Digital recorders, iPods, etc..

Investigators

Electronic crime investigators are trained law enforcement officers with a knowledge of electronic crimes and electronic evidence.

Investigators must have enough technical skill to:

- Gather evidence: Both traditional and electronic
- Comprehend the crime: Understand it is a cybercrime
- Communicate with Technical Experts: Must be able to initiate and understand a discussion of technical nature.

**Importantly, Investigators do not need extensive theoretical knowledge or daily experience with computer systems.

More than anything they must have a solid basic understanding of technical issues, not know how to make everything work

Forensic Analyst

Some large local agencies and many federal agencies have forensic analysts on their payroll.

These individuals are similar to CSI, in that they are the ones who collect a lot of the digital evidence in a cyber investigation.

While investigators are the ones in charge of managing an investigation, the process of actually analyzing the computer evidence is up to the forensic analyst.

This requires a great deal of knowledge of the latest techniques and technologies as well as how tp present findings in court in a coherent manner.

Often involves completing actual training and becoming a subject matter expert to be qualified for court.

Private Police

Also known as corporate security, these individuals have a very different purpose than normal police.

They focus on the good of the corporation, which can sometimes be at odds with the work of the police.

While they strive to cooperate with police, they often end up at odds with police over corporate secrecy and security issues.

Some corporations keep police on staff to advise them about whether or not to call the police.

* Adverse publicity

* Fear of “seize everything” tactics of police

Private police often act as corporate liaison between police and companies in order to keep abreast of their own interests.

Guidelines for Searches and Seizures

Questions to ask about the computer when determining search and seizure issues.

1. Is the computer contraband of Fruit of the Crime: IS the hardware or software stolen.
2. Is the computer a tool of the offense: Was the computer used to commit the crime.
3. Is the computer only incidental to the arrest: Drug dealer maintain trafficking records.
4. Is the computer both instrumental to the offense and storage device for evidence: Used to hack into systems and steal data which is stored on computer.

Guidelines for Searches and Seizures

Once the computer's role is understood, the following essential questions should be answered:

- Is there probable cause to seize hardware?
- Is there probable cause to seize software?
- Is there probable cause to seize data?
- Where will this search be conducted?

Is it practical to search the computer system on site or must the examination be conducted at a field office or lab?

If law enforcement officers remove the system from the premises to conduct the search, must they return the computer system, or copies of the seized date, to its owner/user before trial?

Considering the incredible storage capacities of computers, how will

Guidelines for Searches and Seizures

Search Warrant issues for Electronic Devices

Searches and seizures are for more than just the hardware, in that they include a search and seizure of:

* Hardware

* Software

* Documentation

* User notes and storage media

* Data on the computer

In getting a search warrant against a service provider you ask for

* Service records, billing records, subscriber information

Seizing Computers

- If computer is "OFF", do not turn "ON".
- If computer is "ON”
    - Stand-alone computer (non-networked)
    - Consult computer specialist
        - If specialist is not available

Photograph screen, then disconnect all power sources; unplug from the wall AND the back of the computer.

- Place evidence tape over each drive slot
- Photograph/diagram and label back of computer components with existing connections.
- Label all connectors/cable end to allow reassembly as needed.
- If transport is required, package components and transport/store components as fragile cargo.

Keep away from magnets, radio transmitters and otherwise hostile environments.

Seizing Computers

Networked or business computers
These are computers that are connected to a network, be it a business or personal network
Similar steps for seizing a stand-alone computer with the exception of:

- Unplug power to the router before unplugging the computer
- Includ the router and modem in with the packaging.

- Make sure that with any computer seizure you document the entire process that you followed in seizing the computer (what did you do first, etc..)

Seizing Computers

Network Server or business network
These are the actual servers that are control the network

Consult a computer specialist
Secure the scene and do not let anyone touch except personnel trained to handle network systems.

Pulling the plug could:

1. Severely damage the system
2. Disrupt legitimate business
3. Create officer and department liability.

Cellphones

Potential Evidence Contained in Wireless Devices

- Numbers called
- Numbers stored for speed dial
- Caller ID for incoming calls
    - Other information contained in the memory of wireless telephones
    - hone/pager numbers
    - Names and addresses
    - PIN numbers
    - Voice mail access number
    - Voice mail password
    - Debit card numbers
    - Calling card numbers
    - E-mail/Internet access information
- The on screen image may contain other valuable information

Cellphones

ON/Off Rule

If the device is "ON", do NOT turn it "OFF".

･Turning it "OFF" could activate lockout feature.

･Write down all information on display (photograph if possible).

･Keep the phone charged, if you cannot keep it charged get it to an expert ASAP

If the device is "OFF", leave it "OFF".

･Turning it on could alter evidence on device (same as computers).

･Upon seizure get it to an expert as soon as possible or contact local service provider.

･If an expert is unavailable, USE A DIFFERENT TELEPHONE and contact 1-800-LAWBUST (a 24:7 service provided by the cellular telephone industry).

･Make every effort to locate any instruction manuals pertaining to the device.

Smart Cards

A plastic card the size of a standard credit card that holds a microprocessor (chip) which is capable of storing monetary value and other information.

Awareness

·Physical characteristics of the card

·Photograph of the smart card

·Label and identify characteristics.

·Features similar to credit card/driver's license.

·Detect possible alteration or tampering during same examination.

Potential evidence from Computer Crimes

This section will discuss what types of evidence you should look for in specific types of computer related crime investigations.

Computer fraud

Child Abuse and pornography

Network intrusion

Financial Fraud and Counterfeiting

E-mail Threats, Harassment, and Stalking

Identity Theft

Homicide

Computer Fraud

- Account data from online auctions
- Accounting software and files
- Address books
- Calendar
- Chat Logs
- Customer information
- Credit card data
- Databases
- Digital camera software
- E-mail, notes, and letters
- Financial and asset records

Child Abuse and Pornography

- Chat logs
- Digital camera software
- E-mail, notes, and letters
- Games
- Graphic editing and viewing software
- Images
- Internet activity logs
- Movie files
- User create directory and file names which classify images
- Other???

Network Intrusion

- Address Book
- Configuration files
- E-mails, notes, and letters
- Executable programs
- Internet activity logs
- IP address and usernames
- IRC chat logs
- Source code
- Text files and documents with usernames and passwords
- Other???

Financial Fraud and Counterfeiting

- Address Book
- Calendar
- Currency images
- Check and Money order images
- Customer information
- Databases
- E-mails, notes, and letters
- False ID
- Financial asset records
- Images of signatures
- Internet activity logs
- Online banking software
- Bank Logs and Credit Card Numbers

E-mail Threats, Harassment, and Stalking

- Address Book
- Diaries
- E-mails, notes, and letters
- Financial asset records
- Images
- Internet activity logs
- Legal documents
- Telephone records
- Victim background research
- Maps to victim locations
- Other ???

Identity Theft

This is such a complicated and involved crime that it covers multiple types of computer related areas

Hardware and Software Tools

- Backdrops
- Credit card reader
- Digital camera and software
- Scanner and software

Identity Theft

Internet Activity related to ID theft

- E-mail and newsgroup postings
- Deleted documents
- On-line orders
- On-line trading information
- Internet activity logs
- Others???

Identity Theft

Identification templates

- Birth Certificates
- Check cashing cards
- Digital photo images
- Driver's license
- Electronic signatures
- Counterfeit vehicle registrations
- Counterfeit insurance documents
- Social security cards
- Others???

Identity Theft

Negotiable Instruments

- Business checks
- Cashier’s checks
- Credit card numbers
- Counterfeit court documents
- Counterfeit gift certificates
- Counterfeit loan documents
- Counterfeit sales receipts
- Money orders
- Others???

Homicide

- Address books
- E-mails, notes and letters
- Financial asset records
- Internet activity logs
- Legal documents and wills
- Medical records
- Telephone records
- Diaries
- Maps
- Trophy photos
- Others???