



# Risk Sensitive Evidence Collection

31st Annual  
Computer Security  
Conference and  
Exhibition

# Purpose of this Presentation

- Posits that current methodologies which focus on collecting entire bit-stream images of original evidence disk are increasing legal and financial risks

# Presenters

- **Erin Kenneally, M.F.S., J.D.** - Forensic Analyst at the San Diego Supercomputer Center, liaises and holds leadership positions with the Computer and Technology Computer High Tech Task Force (CATCH) and High Technology Computer Investigation Association (HTCIA)
- **Christopher L. T. Brown, CISSP** - Founder and CTO of Technology Pathways, LLC, Lead architect of the ProDiscover family of computer forensics products

# Agenda

- The first section frames the debate and change drivers for a risk sensitive approach to digital evidence collection.

# Agenda (2)

- Section two outlines the current methods of evidence collection along with a cost-benefit analysis.

# Agenda (3)

- Section three describes the methodology requirements of the risk sensitive approach to collection, and then concludes with a legal and resource risk assessment of this approach.



**Balancing the Risk:  
Refining Collection  
Methodology Without  
Compromising Forensic  
Principles**

# Methodology & Tool Evolution

- Forensic techniques must be evaluated when:
    - dynamic variables
      - data volume
      - business environment
      - legal restrictions
- ...converge to impede the goal of producing verifiable results.

# Modification

- Modifying current digital forensic techniques
    - identification
    - acquisition
    - preservation
    - Analysis
    - presentation
- ... in response to changing contexts does not necessarily mean that results are less reliable for forensic proof purposes.

# contexts

- Addresses the risks of Insisting on bitstream imaging:
  - Large volume (200 GB and above)
  - Time-sensitive
  - Network based S&S

# Current Process: Primary Risk

- Cost Metrics
  - Time
  - Resources
- Both costs are becoming unmanageable

# Computer forensic autopsies

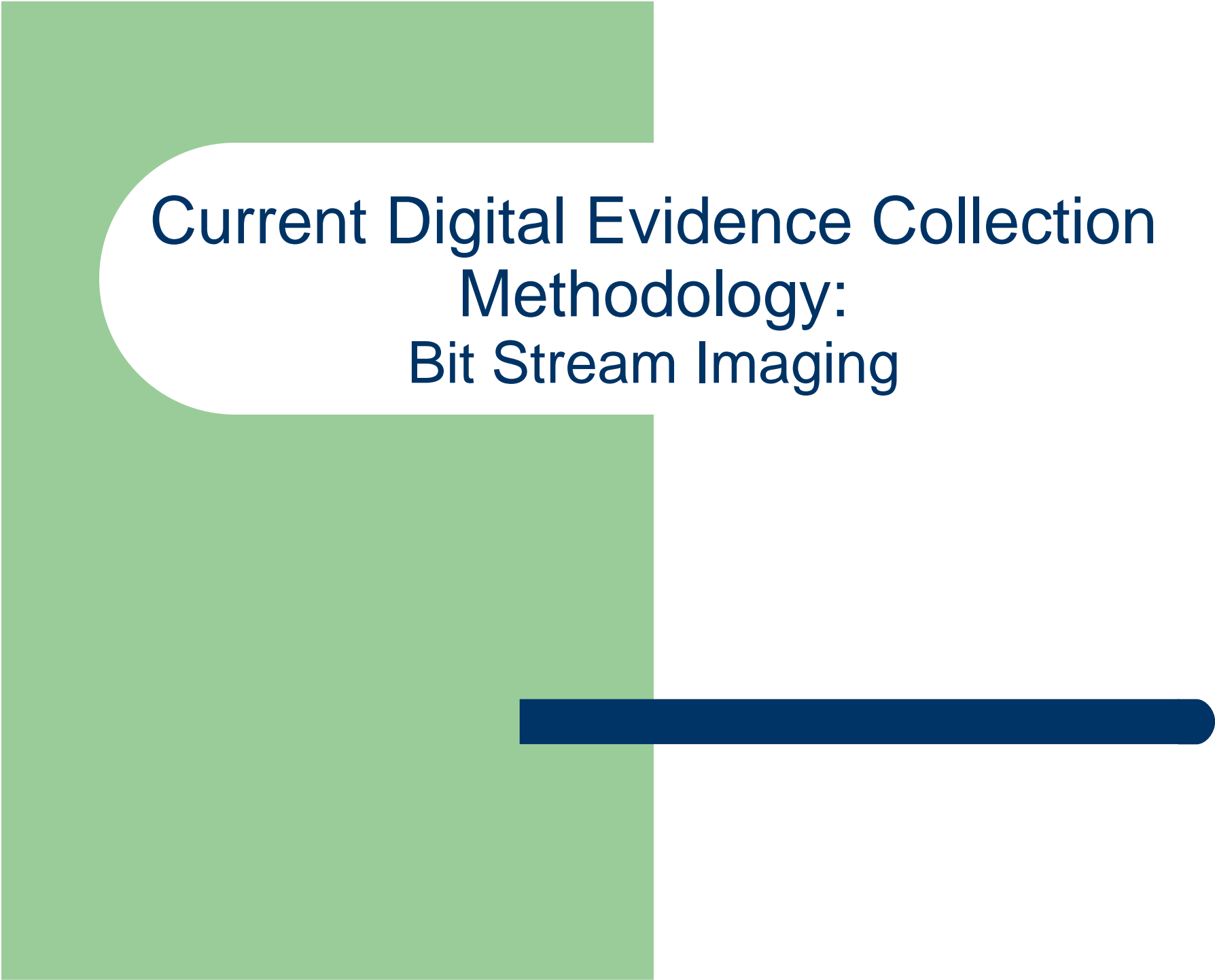
- Past:
  - Single systems with single small capacity disks
- Today:
  - Multiple Systems with multiple large capacity disks and network storage

# Reasonableness

- Cost factors must be managed
  - Legal standards of “reasonableness”
  - Weigh cost & capabilities
  - Does not require perfection

# Net Requirement

- Revised computer data evidence collection methodology is needed which:
  - Balances time and resource cost
  - Meets evidentiary demands of
    - Reliability
    - Completeness
    - Accuracy
    - Verifiability



**Current Digital Evidence Collection  
Methodology:  
Bit Stream Imaging**

# Nature of Digital Evidence

- Collection
  - Complex
  - Volatile
- Direct Analysis
  - Destructive
- Drives the desire for investigators to not perform analysis on original evidence

# Collect Now Analyze Later

- Nature of digital evidence drives desire to collect Everything now and analyze later
- Also helps counter opponent's challenges that LE is deliberately hiding exculpatory evidence.

# Bit-Stream Image (1)

- Copying all data from the original disk
- sector-by-sector
- Image to target working disk or image file
- If the target is a disk then any extra sectors will be written with a known pattern for identification as non-evidence data

# Bit-Stream Image (2)

- Other recommended and accepted techniques Include:
  - Hardware write-blocking
  - Error recovery
  - Error logging
  - Cryptographic HASH Verification

... *help to fortify evidentiary standards*
- All outlined in NIST Disk Tool Specification 3.1.6

# Analysis

- All analysis can be performed on the *image* thus protecting the original evidence disk
- Note that extensive time is spent in disk image analysis in the process of filtering out non-relevant data

# Current Imaging (1)

- Benefits
  - Related/proportional to the size of the target disks
  - Freeze the entire scene as it exists
  - Compartmentalizes the acquisition & analysis

# Current Imaging (2)

- Costs
  - 100 GB IDE ~ 4 hrs.
  - 6,478,200 Microsoft word documents in 100 GB
  - Lost productivity, lost revenue, and soft costs
  - A recent 22 hour outage on EBay's cost the company more than \$5 million in returned auction fees
  - Forrester research estimates the average cost of e-commerce site downtime at about \$8,000 per hour.



**Responding to Change:  
Risk Sensitive Digital Evidence Collection  
Methodology**

# The Methodology

- The Risk Sensitive Digital Evidence Collection Methodology calls (allows) for:
  - Live system evidence identification
  - Selective artifact extraction

while allowing the original systems to continue operating as usual

# Critical Components

1. Live searching and subsequent identification of evidence (pre-search)
2. Selective extraction of low-level evidence supporting artifacts from the digital media

# Live Search and Identification (1)

- Data Connection:
  - Client-server (TSR or Baseline Install)
  - Launch from Read-Only memory
  - Disk sector redirection
  - Other complex tasks as needed
  - Checksums/Encryption for integrity/security

# Live Search and Identification

## (2)

- Data Security:
  - Logical data protection measures provided by the host operating system
  - Logical data protection measures provided by the network environment
  - Physical data protection measures provided by the local environment
- New or existing formalized security audits assist data security component

# Understanding Security Environment

- Allows follow-on analyst to truly understanding evidence during the analysis phase once removed from its native environment.
- Allows investigator to establish which tools and measures should be take to ensure data integrity and security during evidence collection.

# Live Search and Identification (3)

- Data Representation:
  - Client application should reconstruct view from raw data accurately
  - Be read-only
  - Indexes should be provided & hashed in MD5 and/or SHA1
  - Digitally time stamped

# Selective Evidence Extraction

- Based on investigator identification of evidence based on search results from:
  - Keyword match
  - Hash comparison
  - Visual inspection

# Extraction Format

- One or both:
  - File Data Unit
    - Contents of file as seen by native operating environment
  - Sector Data Unit
    - Binary and/or ASCII representation

# Mandatory Supporting Artifacts (1)

- File Data Unit:
  - Metadata
  - Original sector locations
  - File hash value in MD5 or SHA1,
  - MAC (last modified, accessed, created)
- Disk Artifacts:
  - Disk manufacture, ID, geometry, label and true feature set if available

# Mandatory Supporting Artifacts (2)

- File System Artifacts:
  - Any file system meta files such as the MFT (Master File Table) in Windows NTFS
  - File tables / File system index including any time stamps and file size information
  - Index should include any recoverable deleted files
- Identity and Access Control Artifacts:
  - File security identification descriptors and remote access control servers, identity management

# Supplemental Supporting Artifacts

- Include operating system specific artifacts such as:
  - Windows event log files
  - Registry
  - Other compound files such as databases (access, oracle and from email servers)
- Real work to be done:
  - Create environmental templates

# Sample Template

<b>Mandatory</b>		
<i>Artifact</i>	<i>Default Location</i>	<i>Notes</i>
Master File Table	First Sector of Partition	If volume is formatted NTFS
Ntuser.dat	\Documents and Settings \<User>	
<b>Supplemental</b>		
<i>Artifact</i>	<i>Default Location</i>	<i>Notes</i>
Security Event Log "SecEvent.Evt "	%System%/System32/Config/	
System Event Log "SysEvent.Evt "	%System%/System32/Config/	


[Example Artifact Template for Windows 2000 Operating System]

# What's Not Collected

- Non-relevant data
- Data normally filtered out during the analysis of a collected image
- Essentially RSEC is a shifting of *filtering* from analysis to collection
- Overall time needed for collection and analysis are reduced



**Risk Assessment:  
The Costs and Benefits of Risk Sensitive  
Forensic Methodology**



# Benefits

- More cost-sensitive
- Reduction in time/resource requirements for:
  - Forensic investigators
  - Victim data holders
- Evidence storage space requirements can be greatly reduced
  - Easing Hardware Cost Demands
- Decrease lost revenue impact to victim
- Additional soft cost likely

# Legal Benefits (1)

- 4th Amendment challenges and violations
  - Standard: narrow, particular, reasonable
  - Search warrant drafting ---> invalidation  
--> evidence elimination
  - “any/all data related to X” ripe for overreaching in network context
- Methodology is responsive to more granular precision

# Legal Benefits (2)

- Sensitive to Due Process requirements
  - Ask the right question: *whether LE is constitutionally bound to “find” all relevant evidence, including exonerative electronic information?*
  - *DP imposes no affirmative duty upon the state to use the best available technology <Youngblood>*
  - *LE only required to preserve evidence under its control, absent bad faith failure to preserve potentially useful evidence no violate DP <St. v. Yates>*
  - *Selective acquisition via transparent methodology elicits knowledge, control, duty*

# Legal Benefits (2,3)

- Con't (Sensitive to DP)
  - Standard is not 'proving a negative', rather, that methodology reduces uncertainty of technique
    - Accuracy of collection and testing establish reliability  
--> inference that 'uncollected' data lack significant exculpatory value
- *Lack of legal guidance favors a practitioner-based, thought-leadership approach*

# Legal Benefits (4)

- *Risk-Sensitive Upholds Forensic Principles*

*1. When dealing with digital evidence, all of the general forensic and procedural principles must be applied.*

*2. Upon seizing digital evidence, actions taken should not change that evidence.*

*3. When it is necessary for a person to access original digital evidence, that person should be trained for the purpose.*

*4. All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.*

*5. An individual is responsible for all actions taken with respect to digital evidence whilst the digital evidence is in their possession.*

*6. Any agency, which is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles.*

# Legal Benefits (5)

- *Where do we turn in absence of precedent on point?*

*-->Analogy: e-Discovery Model*

*Evidentiary obligations of Preservation Duty  
& Risk Sensitive Evidence Collection*

- *e-Discovery standards derived from same context (resource pressures, reliability requirements)*
- *e-Discovery principles promoted in Risk Sensitive Evidence Collection Methodology*

# Legal Benefits (5) *(Model Principles, con't)*

- (1) Cost-benefit framework
  - a. *<Zubulake>- define scope of discovery limits to minimize cost and balance fairness*
    - *accessible, inaccessible labels*
  - b. FRCP- *construed and administered to "to secure the just, speedy, and inexpensive determination of every action"*
  - c. FRE *construed with business in mind*
  - d. Search warrant *scope narrowness*

# Legal Benefits (5) *(Model Principles, con't)*

- *(1) Cost-benefit framework*

## *e. Sedona Principles*

*“When balancing the cost, burden, and need for electronic data and documents, courts and parties should apply the balancing standard embodied in embodied in Fed. R. Civ. P. 26(b)(2) and its state law equivalents, which requires considering the technological feasibility and realistic costs of preserving, retrieving, producing and reviewing electronic data, as well as the nature of the litigation and the amount in controversy.”*

# Legal Benefits (5) *(Model Principles, con't)*

- *(2) Reasonableness*

- a. FRCP *(proposed)*

- *no duty to retrieve data not reasonably accessible*

- b. *<Zubulake>*

- "Must a corporation, upon recognizing the threat of litigation, preserve every shred of paper, every email or electronic document, and every backup tape? The answer is clearly, 'no.'"*

- c. Sedona Principles

- "..unreasonable to expect parties to take every conceivable step to preserve all potentially relevant data."*

- *deference to reasonable sampling, searching, and*

- selection criteria that determines what is ultimately collected*

# Legal Benefits (5) *(Model Principles, con't)*

## *(3) Flexible Methodology*

- procedures should be responsive to*
  - particulars of evidence*
  - issues of case*
  - technologies involved*

# Potential Costs

- 1. Principles-based challenge:
  - Accuracy, completeness, verifiability, reliability challenges
  - Affect admissibility/weight
  - Convergence of traditional methodology:
    - Collect bit-stream, static
    - Search image file
    - Extract artifacts (iterate)

# Potential Costs

- 2. Due Process Challenges - LE Duty to Collect
  - Fairness tests
    - Gov't duty to preserve "material exculpatory" evidence <*Brady, Agurs*>
    - Bad faith if potentially useful <*Youngblood*>
      - *Application: no precedent in this context, but analogize*
        - *No DP violation when LE fail to preserve breath samples in accordance w/ normal practice <California v. Trombetta>*
        - *DP violation when clothing material to misidentification defense destroyed <US v. Mclure>*



# CONCLUSION

(c) 2004 Kenneally/Brown

# Scope of LE Duty

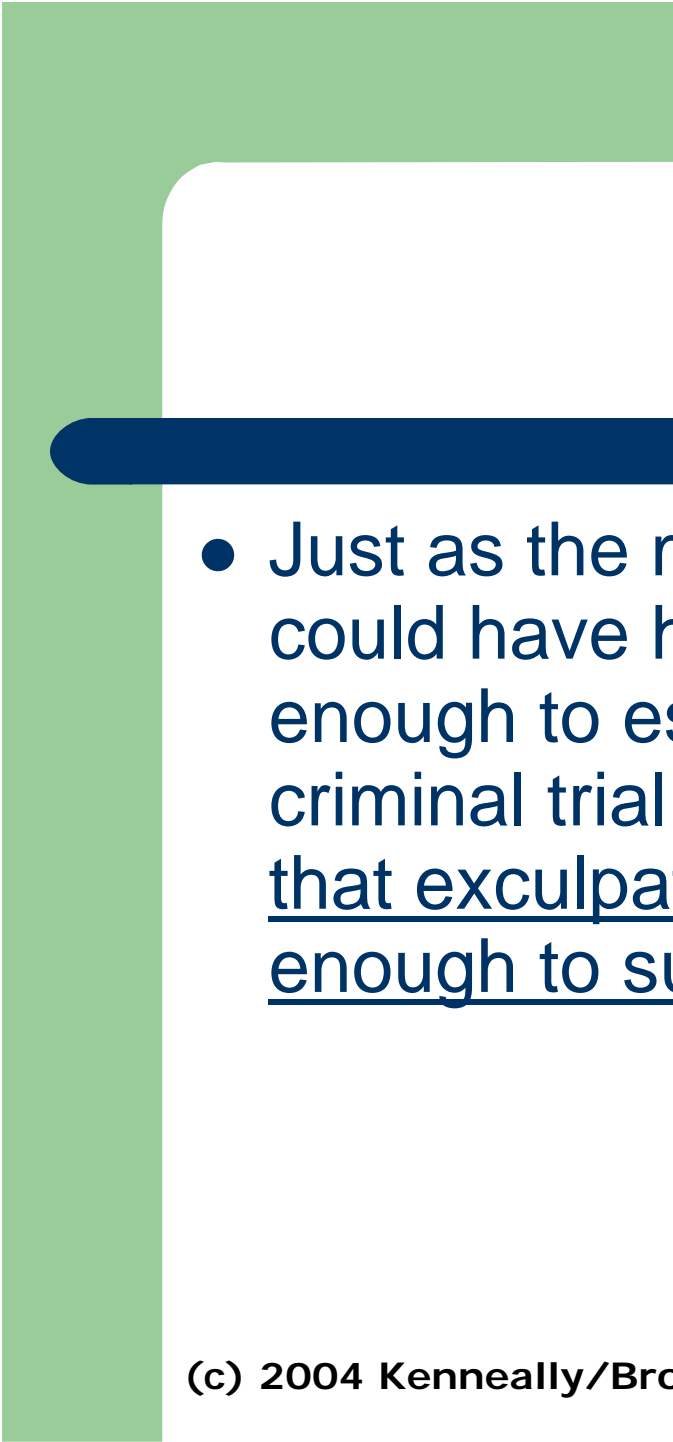

- Risk Sensitive Model : LE is not actively “creating” evidence , but rather, is passively serving as bailor of existing evidence
- *Case law supports collection procedures where the process/results cannot be recreated after the fact.*
- Accuracy and consistency of methodology counter challenges

# The Same, Only Different

- Current v. Risk-Sensitive evidence collection-  
different methodologies but SAME principles
  - Reasonableness
  - Relevance
- Formalizing a methodology to do what is  
often already done in practice benefits all

# Challenges

- Tools to perform RSEC are emerging
- Developing the tools and the training to allow investigators to identify and collect relevant digital data reducing the overall risk of oversight

- 
- 
- Just as the mere possibility that something could have happened is not, in and of itself, enough to establish reasonable doubt in a criminal trial, so too is the mere possibility that exculpatory evidence was not acquired enough to support a due process challenge

# References

- Kenneally, Brown, “Risk Sensitive Digital Evidence Collection”, International Journal of Digital Investigation (forthcoming, Winter 2004).
- The NIST Disk Imaging Tool Specification 3.1.6 describes technical details of recommended processes uses in bit-stream imaging.
- *California v. Trombetta*, 467 U.S. 479, 485 (1984)
- *United States v. Valenzuela-Bernal*, 458 U.S. 858, 867 (1982)
- *United States v. Agurs*, 427 U.S. 97, 49 L. Ed. 2d 342, 96 S.Ct. 2392 (1976)

# References (2)

- *Brady v. Maryland*, 373 U.S. 83, 10 L. Ed. 2d 215, 83 S. Ct. 1194 (1963)
- *Arizona v. Youngblood*, 488 U.S. At 57
- *People v. Eagen*, 892 P.2d 426, 428-29 (Colo. Ct. App. 1994)
- *State v. Yates*, 64 Wn. App. 345, 351, 824 P.2d 519
- *Commonwealth v. Small*, 741 A.2d 666 (Pa. 1999)
- *United States v. Bagley*, 473 U.S. 667 (1985)
- *McCune v. City of Grand Rapids*, 842 F.2d 903, 907 (6th Cir. 1988)

# Thank You!

- Questions?
- Don't forget the feedback sheets