

# The Paralegal's Essential Guide to Electronic Discovery and Computer Forensics



Presented by:  
Ross L. Kodner, Esq.  
*MicroLaw, Inc., Milwaukee*

Sponsored by:  
Paralegal Association  
of Wisconsin  
Milwaukee, Wisconsin  
April 20, 2005  
12PM

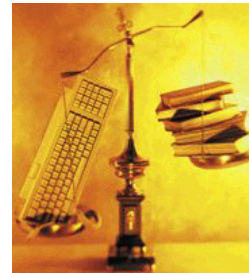


*Special Thanks to:*  
Bruce A. Olson, Esq.  
*Davis & Kuelthau, Green Bay*  
E. Kelly Hansen  
*Neohapsis, Milwaukee/Chicago*

The Paralegal's Essential Guide to Electronic Discovery and Computer Forensics  
©2005, Bruce Olson, Ross Kodner, Kelly Hansen, All Rights Reserved

These materials will be available online at:

[www.microlaw.com](http://www.microlaw.com)



Look for the Paralegal Association links!



The Paralegal's Essential Guide to Electronic Discovery and Computer Forensics  
©2005, Bruce Olson, Ross Kodner, Kelly Hansen, All Rights Reserved

## Your Presenter:

**Ross L. Kodner, Esq.**  
 CEO/Senior Legal Technologist  
 MicroLaw, Inc.  
 Milwaukee, Wisconsin  
 E-Mail: rkodner@microlaw.com  
 Web: www.microlaw.com  
 414.540.9433



- Marquette Univ. Law School, 1986 (Law Review)
- Founded MicroLaw in 1985
- Legal Technologist
- Chair, Milwaukee Bar Association Technology Committee, Chair Wisconsin/Midwest Law & Technology Conference 2002-2005
- Technolawyer Consultant of the Year 1999, Contributor of the Year 2001, 2002
- Over 800 law practices assisted
- Developer of the "Paper LESS Office™" process
- Obsessive author and speaker nationwide on legal technology subjects with over 1200 presentations including dozens for ALA Annual and Regional meetings
- Chair, ABA LPM Section Computer & Technology Division since 1998 and Member, TECHSHOW 1998-2001 Board; Co-Chair, LegalTech Planning Board; LegalWorks Planning Board
- Former Board Member, State Bar of Wisconsin Law Practice Section; Technology Resource Committee
- Co-Founder, Legal Technology Alliance

The Paralegal's Essential Guide to Electronic Discovery and Computer Forensics  
 ©2005, Bruce Olson, Ross Kodner, Kelly Hansen, All Rights Reserved

## Special Thanks To:

**Bruce A. Olson, Esq.**  
 Shareholder / Litigation & Discovery Counsel  
 Davis & Kuelthau, S.C.  
 Green Bay, Wisconsin  
 E-Mail: bolson@dkattorneys.com  
 Web: www.dkattorneys.com  
 920.431.2230



- Marquette Univ. Law School, 1981
- Board Certified Civil Trial Specialist by National Board of Trial Advocates 1997, recert. 2002
- AV Rated Martindale-Hubbell
- 2002 TechnoLawyer of the Year
- Chair ABA TECHSHOW 2004
- Vice Chair ABA TECHSHOW 2003
- ABA TECHSHOW Board 2001-2004
- ABA Law Practice Management Board 2004 – present
- Nationally recognized legal technologist, author and presenter
- President of ONLAW Trial Technologies, LLC

The Paralegal's Essential Guide to Electronic Discovery and Computer Forensics  
 ©2005, Bruce Olson, Ross Kodner, Kelly Hansen, All Rights Reserved



## Special Thanks To:

### E. Kelly Hansen

CEO  
Neohapsis, Inc.  
Milwaukee, Wisconsin & Chicago, Illinois  
E-Mail: khansen@neohapsis.com  
Web: www.neohapsis.com  
414.289.0966



- Neohapsis is a leading information security consultancy and IT security product test lab
- Neohapsis is the primary security test lab for Network Computing & Secure Enterprise magazines.
- Hansen is a regular columnist Secure Enterprise magazine
- Opened forensics practice in 1999 and have worked on over 200 cases to date.
- Recently brought on Dave Stampely, former asst. AG NY to run compliance & privacy program



## Special Thanks Also To:

John Simek and  
Sharon Nelson  
Sensei Enterprises  
Fairfax, Virginia



## Important Disclaimer

- A speaker's opinions are just that - opinions
- Not offering legal advice – just discussing principles
- Any questions from audience welcome, but any replies are general comments only and should not to be construed as legal advice



## Overview of Electronic Discovery

- Difference between Traditional Discovery and E-Discovery
- Same basic legal rules and concepts
- What are we looking for – anything that is reasonably calculated to lead to
- Relevant evidence at trial
- Electronic information is content +
- Traditional information is simply content



## Overview of Electronic Discovery

---

- **Why is E-Discovery an Issue?**
- **Increased use of computers generating electronic data that may or may not be reduced to paper at every level of society**
  - **Businesses**
  - **Governments**
  - **Individuals**



## Overview of Electronic Discovery

---

- **Why is E-Discovery an Issue?**
- **Widespread use of computers brought new technologies –**
  - **Email**
  - **Voicemail**



## **Overview of Electronic Discovery**

---

- **Ability to share vast amounts of information instantaneously over the Internet**
- **Explosion of instantaneously available and searchable information**



## **Overview of Electronic Discovery**

---

- **Information Explosion**
  - **The world produces between 1-2 exabytes of unique information each year**
  - **1 exabyte = 1 trillion books**
  - **Of this information, only .003 % is printed**



## Overview of Electronic Discovery

- **Information Explosion**
  - **Small percentage of new information is paper based**
  - **Recorded information – 97% created electronically**
  - **Corporate information – 80% or more now exists only in electronic form**
  - **Corporate communications – 30% or more never reduced to paper**



## Overview of Electronic Discovery

- **Information Explosion**
  - **Email**
  - **65% never printed**
  - **1 million messages sent every hour**
  - **1 in 20 companies have battled a workplace lawsuit triggered by e-mail**
  - **Exponential growth in court or other regulatory body ordered production of email**



## Overview of Electronic Discovery

---

- **Scope –**
  - **Who does it affect?**
  - **Everyone!**



## Overview of Electronic Discovery

---

- **Scope –**
  - **Convergence of IT, Records Management and Legal personnel**
  - **Higher level of sophistication and understanding of cross-disciplinary issues**
  - **Requires greater collaboration and cooperation than in the past**



## Overview of Electronic Discovery

---

- **Scope -**
  - **What is included?**
  - **Paper managed electronically**
  - **Electronic information that never becomes paper**



## Overview of Electronic Discovery

---

- **Scope - Different types of E-Discovery**
- **Forensic Discovery**
- **Substantive Discovery**
  - **Technical**
  - **Conventional**



## Overview of Electronic Discovery

- Consequences of poor management:
  - SPOILIATION of EVIDENCE
  - Spoliation leads to:
    - DRACONIAN PENALTIES
    - Absence of key evidence at trial
    - Financial sanctions
    - Dismissal of case
    - Attorney malpractice



## Overview of Electronic Discovery

- Spoliation of Evidence -
  - *“The destruction or significant alteration of evidence, or the failure to preserve property for another’s use as evidence, in pending or future litigation.”*



## Overview of Electronic Discovery

- **Spoliation of Evidence**
  - Inadvertent destruction
  - Intentional destruction
  - Inadequate document retention policies



## Overview of Electronic Discovery

- **Good records management:**
  - Anticipates litigation is inevitable
  - Has a heightened awareness of potential adverse consequences of improper management
  - Adopts an effective plan
  - Ensures that plan and procedures are followed, maintained and updated over time

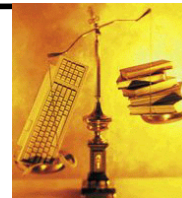


## Overview of Electronic Discovery

- Who needs to be aware of these issues?
  - IT
  - Executives
  - Management
  - Key employees at all times
  - All employees when litigation is anticipated



## Electronic Discovery Primer (and Data Collections Methods and Risks)



- The Technical and Legal Aspects of  
Electronic Discovery Now and in the Future



## Electronic Evidence—Why Care?

- ***“Today it is black letter law that computerized data is discoverable if relevant.”***

*Anti-Monopoly, Inc. v. Hasbro, Inc.*, 94 Civ. 2120, 1995 WL 649934 (S.D.N.Y., November 3, 1995)



## Electronic Evidence—Why Care?

- **Over 93% of documents are electronic**
- **Most will never become paper**
- **North America sends more than 4 trillion e-mails per day**
- **Average non-spam per worker: 20-60 e-mails per day**
- **Discovery routinely includes electronic documents**



## Electronic Evidence—Why Care?

- Document retention policies often don't exist
- Document retention policies often aren't enforced
- 10% of employees will ignore compliance orders
- If your servers/workstations won't kill you, your back-up may
- Preservation of evidence letters put you on notice and spoliation penalties increasingly severe



## Electronic Discovery Today

- Revenues in 1999: \$40 million
- Revenues in 2003: \$430 million
- 60% increase over 2002
- 60% increases predicted for next 3 years
- 67 new companies in 2003



## Market Leaders (36% overall)

- Cricket Technologies
- Daticon
- Electronic Evidence Discovery, Inc.
- Kroll Ontrack, Inc.
- Lexis-Nexis Applied Discovery



## Recoverable (if not overwritten!)

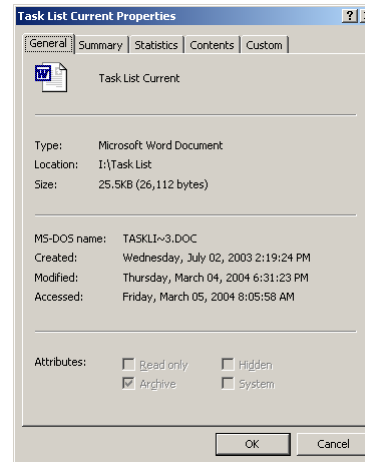
- Deleted files and Metadata
- Internet history and "cache" files
- ICQ "conversations"
- E-mail
- Installed applications and data
- Computer activity timeline
- Files where extensions are intentionally modified
- PDA data
- Digital media cards





## The Metadata Threat

- Data About Data
- Word
- WordPerfect
- Excel
- PowerPoint
- Scrubbers
- Metadata Assistant
- Copy & Paste (Special)



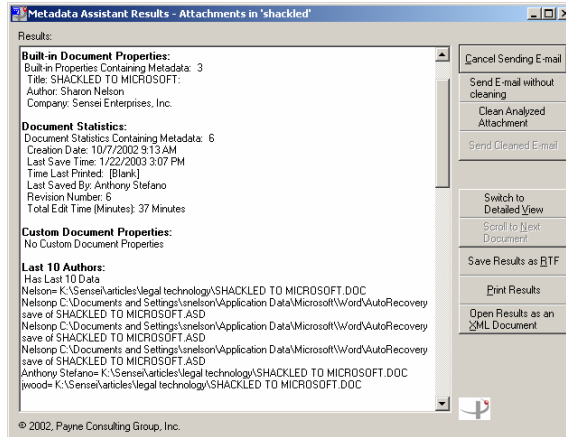
## Technical

### Where does evidence hide?

- Metadata
- Is data embedded in the file that details, describes, gives more attributes about the file.
- A Microsoft Windows computer typically has dozens of applications installed, each performing different tasks that save data to the hard-drive in different formats.
- Many applications have hidden embed data

## Metadata Assistant

From Payne Consulting ([www.payneconsulting.com](http://www.payneconsulting.com))  
and available through MicroLaw, Inc. in Wisconsin




## Technical

### Where does evidence hide?

- Metadata - Example
- The "GOOD MORNING" text file and the "GOOD MORNING" Microsoft Word file display exactly the same text when opened, yet these files are significantly different in size.

MICROLAW  
Lawyers Helping Lawyers Since 1982  
Technology Since 1982  
www.microlaw.com

Paralegal Association of Wisconsin Educational Seminar  
Presented by: Ross L. Kodner, Esq.



## Technical

Volume in drive A has no label  
Volume Serial Number is 18E8-0D50  
Directory of A:\


GOODMO~1 TXT	13	06-07-02 5:07p
Good morning.txt		
GOODMO~1 DOC	19,456	07-30-02 3:56p
Good Morning.doc		
GOODMO~1 PGP	575	06-07-02 5:25p
Good morning.txt.pgp		
GMLINK TXT	1,703	06-08-02 10:23a
GMLINK.TXT		
DEOFTXT TXT	462	06-08-02 10:36a
DEOFTXT.TXT		
DESLACK TXT	213	06-08-02 11:28a
Deslack.txt		
6 file(s)	22,422 bytes	
0 dir(s)	1,433,600 bytes free	

The Paralegal's Essential Guide to Electronic Discovery and Computer Forensics  
©2005, Bruce Olson, Ross Kodner, Kelly Hansen, All Rights Reserved

35

MICROLAW  
Lawyers Helping Lawyers Since 1982  
Technology Since 1982  
www.microlaw.com

Paralegal Association of Wisconsin Educational Seminar  
Presented by: Ross L. Kodner, Esq.



## Technical

### Where does evidence hide?

- **Meta-Data - Example**
- The difference in size of the two files is a result of “meta-data” hidden within the file.
- Meta-data contains time/date stamps of a file:
  - **Creation**
  - **Access**
  - **Modification**
- In a typical Microsoft Word file meta-data may include:
  - **Author**
  - **Number of revisions**
  - **Time and date of the last time the document was printed**

The Paralegal's Essential Guide to Electronic Discovery and Computer Forensics  
©2005, Bruce Olson, Ross Kodner, Kelly Hansen, All Rights Reserved

36



## Technical

### Where does evidence hide?

- Meta-data - EMF
- When a computer user prints a file, regardless if it is a Word document or a web page, the computer rarely sends text to a printer; rather it sends a graphic representation of the file.
- This graphic representation is called an enhanced metafile (EMF), and it is written to the disk usually in a temporary directory.
- After the file is successfully printed, the EMF is deleted by the operating system.
- The EMF may be the only evidence of the document's existence and may become a vital piece of evidence when files are printed from removable media, such as a floppy diskette.



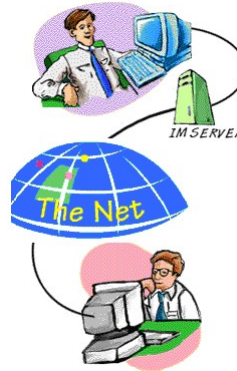
## Technical

### Where does evidence hide?

- Metadata - Link Files
- Link files are pointers to other files and they contain meta-data. The meta-data contains information about the referenced file.
- In the "GOOD MORNING" example, the Windows 98 operating system created a link file that showed the path to where the file was saved (A:\Good Morning.doc).
- The fact that the file was saved to the A: drive may be the critical piece of evidence to substantiate theft of data.
- A link file has it's own creation, modification and access
- Volume labels could identifies floppies, drives

## Unrecoverable

- Wiped drive areas
- Instant Messaging
- Overwritten files (maybe . . . )
- Frequently, segments of files
- Encrypted files



## The Day You Learn Your Client May Be Sued

- Forward any Preservation of Evidence Letter or notice from the other side
- Write your own Notice to Client
- Prepare a memorandum to be circulated to all involved parties on your side
- Explain spoliation and its consequences
- Advise client not to look for evidence itself



## The Day You Learn Your Client May Be Sued

---

- Cease overwriting backup media
- If a particular machine or machines are in issue, unplug them and keep them under lock and key
- Advise client not to defrag, compact, load new applications, delete applications, or get rid of computers
- Warn client about peripheral devices
- Don't get rid of machines or swap out HDs



## Why Not Look Yourself or with Your IT Staff?

---

- Just booting a computer changes hundreds of file access times
- Potential compromise of timeline by changing date
- Shutdown and startup process vary by system configuration
- Overwrite swap file area
- Evidence may become suspect or rendered inadmissible



## Preservation of Evidence Letter

- Put other side on notice – avoid spoliation
- Specify all media
- Specify all locations
- Specify nature of evidence
- Specify particular individuals



## Preservation of Evidence Letter

- No deletion, moving or modification of discoverable evidence
- Machines with discoverable data
- No defragging
- No new applications loaded
- No new data / no modified data
- No disk optimization
- No Metadata scrubbing/removal



## Preservation of Evidence Letter

---

- **No overwrite of backup media**
- **No disposal of machines or media**
- **Obtain protective order if necessary**



## Protective Orders

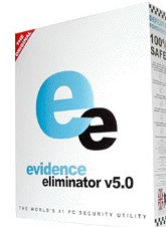
---

- **Enron shredding/Andersen deletions**
- **Protective Order by agreement preferable**
- **Likelihood that evidence will be destroyed**
- **Indicia of bad faith**
- **Prior history of spoliation**
- **Be very specific**



## Wiping and Scrubbing

- Evidence Eliminator
- Evidence Scrubber
- Disk Wiper
- All leave traces
- Spoliation is both damning and expensive



## Gaining Access to E-Evidence

- By agreement
- Request for Production of Documents
- Motion to Compel
- Identify what is to be accessed
- Narrowness and relevance of search
- Not unduly burdensome
- Subpoena to ISP



## Computer Protocol Agreement

- Where will acquisition take place? ASAP to avoid destruction/trampling. Dates?
- On-site Inspection
- Privilege? Producing party can screen first
- Non-waiver Agreement
- Can define terms of search – keywords, dates etc.
- Confidentiality Agreement
- Destruction at end of case – return to owner?
- Child Porn Protocol



## Discovery – Interrogatories and Depositions

- Be specific – not overbroad
- Use keywords, date ranges, specific individuals, etc.
- OS?
- Firewall?
- Network? How configured?
- Class of machines?
- Applications?

## Discovery

- How does backup work?
- When is media overwritten?
- System admin?
- PDA? Laptops? Home machines?
- Cell phones? Digital copiers? Thumb drives?
- Remote access? How?
- E-mail package?
- E-mail server?
- Where is e-mail stored?



## Depose IT Staff

- Ask all the same questions
- Verify all previous answers/get details
- Logging?
- Monitoring?
- Security structure?
- User IDs/passwords, e-mail addresses
- Encryption program? Get keys



## Depose Individuals

---

- Do they do their own backups?
- Do they make copies?
- Identify personal computing habits
- What applications do they use?
- Which machines at work do they use?
- Home computer? PDA? Laptop?
- Cell phone? Pager? Thumb drives?



## Costs

---

- Who pays for computer forensics?
- Typically, producing party pays
- Party seeking discovery may offer to pay
- Courts consider resources of producing party and extent of burden
- Our costs, by way of example: \$1000 per HD imaged, \$280/hr. for analysis/testimony





## **Cost Shifting: Zubulake v. UBS Warburg**

---

- **Cost must normally be borne by producing party**
- **New seven factor test established by court**
- **This decision appears likely to become the “gold standard”**



## **Zubulake v. UBS Warburg**

---

- **Extent to which request is tailored to discover relevant info**
- **Available from other sources**
- **Cost of production compared to amount in controversy**
- **Cost of production compared to each party's resources**



## Zubulake v. UBS Warburg

---

- Ability and incentive of each party to control costs
- Importance of the issues at stake
- Relative benefits to the parties of obtaining the information requested
- Zubulake III permitted “sampling” to limit costs



## Data Collection

---

### Computer Forensics

- What is it?
  - Computer forensics is the practice of identifying, preserving, analyzing, recovering, and presenting potential electronic evidence.
  - It involves supportive measures such as incident preparation, detection, response and remediation.
  - The principal function of computer forensics is the investigation of alleged computer-related policy infractions, abuses and crimes.



## Data Collection

---

### Computer Forensics

- What is it?
  - Organizations use computer forensics to conduct investigations into both internal and external computer related incidents. A computer forensic investigation may range from tracking down a hacker on a system to recovering inappropriate emails to unearthing evidence of fraud.



## Data Collection

---

### What is Computer Forensics?

- Litigation Support & Consultation
- Evidence Acquisition & Archival
- Forensic Analysis
- Expert Witness Testimony



## Data Collection

---

### What can you find?

- Deleted information
- Hidden data
- Logs
- Internet cookies
- Sites visited
- Cached files
- Documents
- Spreadsheets
- Letters
- Memos



## Data Collection

---

### What can you find?

- Encrypted data
- Metadata
- Within JPG (e.g. thumbnails), word docs (e.g. time/date stamps)
- Email
- Contact information
- Correspondence
- Temporary files
- Financial information and transactions
- Trojans
- Pirated software
- Graphics

MICROLAW  
Lawyers Helping Lawyers Since 1982  
Technology Since 1982  
www.microlaw.com

Paralegal Association of Wisconsin Educational Seminar  
Presented by: Ross L. Kodner, Esq.

63

## What a Forensic Technologist Brings

- Knowledge of multiple operating systems and procedures
- Hardware and software tools to recreate environment
- Lots of drive space
- Maximize evidence retrieval
- Case roadmap/next steps
- Expert witness credentials
- Proof of chain of custody/authentication

The Paralegal's Essential Guide to Electronic Discovery and Computer Forensics  
©2005, Bruce Olson, Ross Kodner, Kelly Hansen, All Rights Reserved


MICROLAW  
Lawyers Helping Lawyers Since 1982  
Technology Since 1982  
www.microlaw.com

Paralegal Association of Wisconsin Educational Seminar  
Presented by: Ross L. Kodner, Esq.

64

## Choosing a Forensic Technologist

- Technical certifications
- Forensic certifications
- Courts qualified
- Professional experience
- Referrals from clients



The Paralegal's Essential Guide to Electronic Discovery and Computer Forensics  
©2005, Bruce Olson, Ross Kodner, Kelly Hansen, All Rights Reserved



## Choosing a Forensic Technologist

---

- CV-get & ask questions
- Seminars & Publications
- Speaks English
- Knowledge of the Law



## Checklist: Working with Your Experts

---

- Get them the pleadings
- Define the scope of their effort ASAP to limit costs
- Involve them in drafting pleadings, sitting in on relevant depositions
- Give them adequate notice of deadlines and court dates



## Checklist: Working with Your Experts

---

- Don't write their opinions
- Accept "the truth" as they report it
- Respond promptly to their messages/queries
- Do not discuss substantive matters via e-mail
- Don't write a "draft" report until discussed by phone



## Substantive Law

---

- *A discovery request aimed at the production of records retained in some electronic form is no different, in principle, from a request for documents contained in an office file cabinet. While the reality of the situation may require a different approach and more sophisticated equipment than a photocopier, there is nothing about the technological aspects involved which renders documents stored in an electronic media "undiscoverable."*

*Linnen v. A.H. Robins Company, Inc.*, 1999 Mass. Super.  
LEXIS 240 (Mass. Super. June 16, 1999)



## Substantive Law

---

- ***“Deleted electronic data is fully discoverable.”***

*Dodge, Warren and Peters Insurance Servs. v. Riley*, E031719, 2003 WL 245586 (Cal. App. February 5, 2003).



## Substantive Law

---

- ***“Computer records including records that have been ‘deleted,’ are documents discoverable under Fed.R.Civ.P.34”***

*Simon Prop. Group LP v. my Simon, Inc.*, 194 F.R.D. 639 (S.D. Ind. 2000)



## Substantive Law

- **Rules 26(c), FRCP, allows the shifting of discovery costs to protect a respondent “from annoyance, embarrassment, oppression or undue burden or expense.”**

*See In re First Am. Corp.*, 184 F.R.D. 234, 239 (S.D. N.Y. 1998).



## Substantive Law

- **Cost Allocation - Under F.R.C.P discovery rules:**
- **Generally, each party bears its own discovery costs. Some courts will not hesitate to place the burden of production on the producing party.**

*Linnen v. A. H. Robbins Company*, 1999  
WL462015 (Mass.Super. June 16, 1999).



## Substantive Law

---

- **Representative Case Law –**
- **Some courts have attempted to reach a compromise between cost allocation and cost shifting. The 7th Circuit, for example, allocated electronic discovery expenses equally among the parties in**

*Sattar v. Motorola, Inc.* 138 F.3d 1164 (7th Cir. 1998).



## Substantive Law

---

- **Preservation Directive –**
  - **When litigation is foreseen or commenced against a company, to avoid any claim of spoliation because of inadvertent destruction of documents, a high management official should notify and formally direct, in writing, employees not to destroy any documents that are potentially related to the litigation and to suspend corporate record retention policies that may relate to scheduled destruction of such documents.**



## Substantive Law

---

- Preservation Directive -
- Additional preservative steps are particularly needed with respect to electronic records, especially e-mail, which may be subject to regular, routine, automated deletion. In some computer systems, if a computer with relevant evidence is even started up or “booted,” certain files (e.g. “temporary files” and “swap files”) may be destroyed.
- Carey Sirota Meyer and Kari L. Wraspir, *E-Discovery: Preparing Clients for (and Protecting them Against) Discovery in the Electronic Information Age*, 26 Wm. Mitchell L. Rev. 939, 961 (2000).



## Substantive Law

---

- Preservation Directive
- See also: United States of America v. Philip Morris USA, et al. , No. 99-2496 (D.C. D. Columbia July 21, 2004) (Court awarded \$2,750,000 as monetary sanction where Philip Morris and Altria Group deleted email over 60 Days old on a monthly, system wide basis for at least two years after the court had issued an order requiring preservation of "all documents and other records containing information which could potentially be relevant to the subject matter of this litigation.



## Substantive Law

- **SPOILIATION**
- **Failure to preserve e-mail and electronic documents (whether intentional or inadvertent) is sanctionable as spoliation of evidence.**

*Metropolitan Opera Assoc. Inc. v. Local 100, 212 F.R.D. 178 (S.D.N.Y. 2003)*



## Substantive Law

- **SPOILIATION**
- **Sanctions**
- **Default judgment**
- **Adverse inferences**
- **Monetary sanctions**
- **Criminal penalties**



## Substantive Law

- **SPOILIATION**
- **See: Zubulake V and United States v. Philip Morris, et al.**



## ED Technology Solutions

- **Electronic discovery solutions and services abound**
- **Companies who manage data capture, data production, data searching, document coding**





## **Emerging ED Concept: “National Discovery Counsel”**

- **The concept is new, the need is real and pressing**
- **A new and emerging category of litigation counsel**



## **Emerging ED Concept: “National Discovery Counsel”**

- **Specialist counsel who works with lead counsel bringing expertise in management of the discovery process**
- **Special expertise in electronic discovery including resource selection, techniques, processes, procedures, cost projection, interface with technical resources**



## **Emerging ED Concept: “National Discovery Counsel”**

---

- **Use attorneys in less expensive markets**
- **One firm develops specialized expertise in your systems**
- **No need to pay to train every new set of lawyers**
- **Collaborate with counsel on technology choices**



## **Emerging ED Concept: “National Discovery Counsel”**

---

- **Coordinate document production procedures and policies for consistency**
- **Work with management to develop e-discovery procedures**
- **Develop legally sound document/data retention, backup, archiving and destruction policies**



## Emerging ED Concept: “National Discovery Counsel”

---

- Work with local trial counsel for discovery related issues
- Prepare responses to e-discovery interrogatories, requests for production of documents
- Defend depositions of company personnel



## Emerging ED Concept: “National Discovery Counsel”

---

- Handle motions to compel or motions for protective orders
- Handle relationships with outside referees, special masters
- Handle relationships with outside vendors



## **Strategies and Solutions**

---

### **Electronically Savvy Litigators or Technopeasants?**

- **The days of technopeasant litigators who proudly profess digital illiteracy are over**
- **How do you assess the technical prowess and comprehensive of your litigation counsel?**
- **What to look for?**
- **What to avoid?**
- **Separating the Pros from the Amateurs**




## **Strategies and Solutions**

---

- **Familiarity of Counsel with Technology:**
- **Know what is out there**
- **Know how to use it**
- **Attorneys must use it regularly**
- **Not a staff function anymore**
- **Don't let them bluff you!**

MICROLAW  
Lawyers Helping Lawyers Since 1982  
Technology Since 1982  
www.microlaw.com

Paralegal Association of Wisconsin Educational Seminar  
Presented by: Ross L. Kodner, Esq.



## Strategies and Solutions

- **Familiarity of Counsel with Technology:**
- **Know how to interact successfully with IT**
- **Know how to work with and foster collaboration with IT and managers**
- **Know how to pursue and protect your information based on technologies in question**

**The Paralegal's Essential Guide to Electronic Discovery and Computer Forensics**  
©2005, Bruce Olson, Ross Kodner, Kelly Hansen, All Rights Reserved

89

MICROLAW  
Lawyers Helping Lawyers Since 1982  
Technology Since 1982  
www.microlaw.com

Paralegal Association of Wisconsin Educational Seminar  
Presented by: Ross L. Kodner, Esq.



## Litigation Support Tools and Non-Legal Approaches

- **Litigation support tools abound for organizing documents, searching your information, managing document storage and retrieval**



SUMMATION  
LEGAL TECHNOLOGIES, INC.





**The Paralegal's Essential Guide to Electronic Discovery and Computer Forensics**  
©2005, Bruce Olson, Ross Kodner, Kelly Hansen, All Rights Reserved

90



## Helpful Resources

---

- [www.krollontrack.com](http://www.krollontrack.com)
- <http://www.applieddiscovery.com/lawLibrary/eDiscoveryPrimer.asp>
- [www.discoveryresources.org](http://www.discoveryresources.org)
- **BNA, Computer Technology Law Report (electronic edition)**
- **Google News Alert - [www.google.com/newsalerts](http://www.google.com/newsalerts)**
- **electronic+discovery**



## Helpful Resources

---

- ***Electronic Discovery and Evidence***
  - **Michael R. Arkfeld**
  - **Law Partner Publishing 2003**

# Thank You For Listening! For Legal and Technology Guidance on Electronic Discovery, I'm Happy to Help . . .

---



**Ross L. Kodner, Esq.**  
President and CEO  
MicroLaw, Inc.  
Phone: 414-540-9433  
E-Mail: rkodner@microlaw.com  
Web: www.microlaw.com

**The Paralegal's Essential Guide to Electronic Discovery and Computer Forensics**

*©2005, Bruce Olson, Ross Kodner, Kelly Hansen. All Rights Reserved*

93