

# **PRACTICAL ADVICE FOR DEALING WITH THE NEW E-DISCOVERY RULES**

**By: Mark Henriques**

**WombleTech 11/15/07**



**WOMBLE  
CARLYLE**  
OUR LAWYERS  
MEAN BUSINESS

## Today we will:

- Discuss some practical impacts of the December 2006 E-Discovery Rule Changes;
- Hear from David McClellan about admissibility challenges to electronic documents.



## **E-Discovery is crucial:**

- Most new cases will involve e-discovery.
- Over 94% of newly created information is stored electronically.
- Malpractice concerns.
- Expensive and time consuming, but source of key discovery.



# Litigation Off Switch

Immediately stop  
deletion of  
email and other  
electronic documents



## Identify the **KEY PLAYERS**



**The Litigation Holds begins with their e-mails,  
documents and data.**



**WOMBLE  
CARLYLE**  
OUR LAWYERS  
MEAN BUSINESS

## **After 12/06, Lawyers Must:**

- Prepare for Initial Attorney's Conference, by obtaining information about client's:
  - Servers.
  - Back up systems and tapes.
  - Storage devices (Palm Pilots, Treos, Thumb Drives, Laptops, etc.).
  - E-mail retention.



## Discuss at Conference

- Time period for electronic discovery.
- Various sources of each party's electronic data (ESI).
- Reasonable accessibility of ESI.
- Preservation of ESI.
- Form of production.
- Privilege issues relating to ESI.



# Email Production Options

(not including privilege search/  
assumes keyword relevancy search)

**Active Files (KVS) – July 2004 to Present                      \$50K**

## Archived files – Jan 2002- June 2004

Option A – Quarterly tapes      80-85%                      \$73K/year              \$182.5K

Option B – Monthly Tapes      91-95%                      \$158K/year              \$395K

## Legacy files – 1999-2001

Option A – Quarterly tapes      80-85%                      \$500K/year              \$1.5MM



## What is Reasonably Accessible ?

- Only need to produce “Reasonably Accessible Data.” Focus on undue burden or cost.
- If data is not reasonably accessible, burden shifts to requesting party.
- Need to show good cause because benefits outweigh costs.



## Judge Scheindlin's Hierarchy

**Most accessible**

**to**

**Least accessible**

Active, online data

Near-line data

Offline storage/archives

Back up tapes

Erased, fragments or  
damaged data



## Amendments to Rules 33(d) and 34

- Requesting party may specify the format for production.
- If no format specified, production should be in the format in which the data is ordinarily obtained or is reasonably useable.
- What about Metadata ?



# E-Mail Options:

## Form

Hard copy print out

Single page TIFF or pdf

Native

## Problems

No Metadata

Loses connection with attachments

Privilege and redaction;  
bates numbering  
difficulties



# Excel Spreadsheets

- Excel spreadsheets are created to be “active” – with cells that can be manipulated, calculated and sorted.
- Static TIFF or hard copy production disables this interaction.
- Williams: Improper to lock cells and scrub metadata.



# Sanctions

- **Most Commonly Sanctioned Behavior:**
  - **Destruction of evidence (84%)**
  - **Delayed production (16%)**
- **Most Common Sanction:**
  - **Attorney's fees and costs are the most commonly granted sanction (60%)**
  - **Evidentiary preclusion (30%)**
  - **Adverse inference instructions (23%)**
  - **Dismissal or default (23%)**





# *Data Authenticity - The NEXT eDiscovery Challenge*

*David McClellan  
VP & GM – Financial Services  
ProofSpace*

*WombleTech Lunch & Learn  
November 15, 2007*



# eDiscovery – Today and Tomorrow

## *Where We've Been*

### ▶ Blocking & Tackling

- Cataloging and indexing data
- Records retention, legal hold, destruction
- Deploying “vaulting” technology

## *Where We're Going?*

### ▶ Authenticity Challenges

- Proving authenticity of ESI
- Authenticity challenges as legal tactic
- Consumers gain leverage against corporations. Settling frivolous claims for 100s of thousands of dollars may become a smart business decision when the consumer's counsel doesn't stipulate out.



# Trust in Corporate America Has Eroded

Enron  
&  
Arthur  
Andersen

Mutual Fund  
Late Trading

Insurance cos.  
falsify claims  
reports to  
avoid paying  
Katrina  
settlements

Rampant  
Earnings  
Restatements

Prosecution of  
Trusted Insiders  
- McAfee  
- Converse  
Technology  
- Etc.

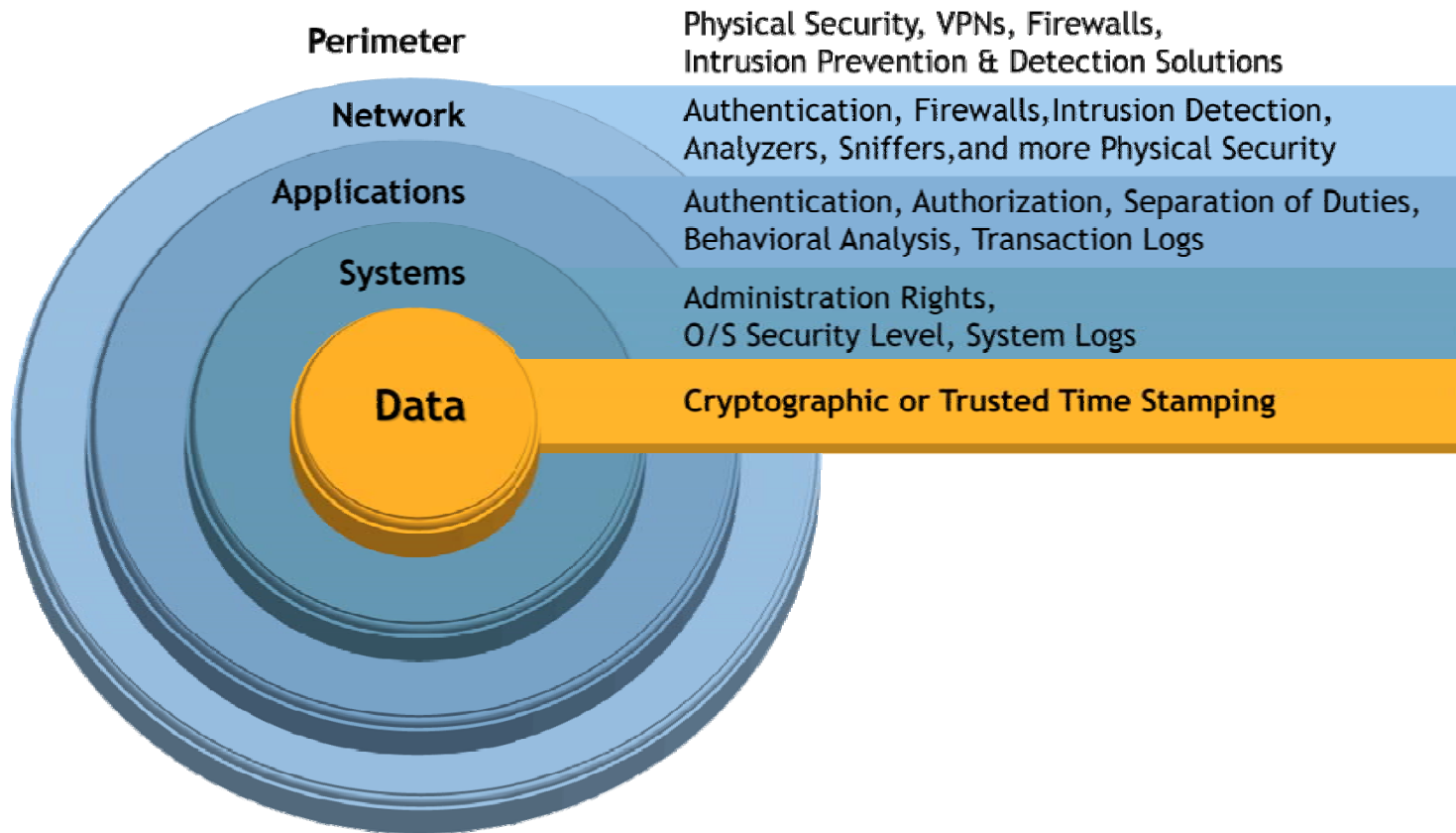
Robins Kaplan  
attorney alters  
documents  
submitted as  
evidence for  
Best Buy

Morgan  
Stanley fined  
\$1.4 billion for  
failure to  
produce email  
records

Options  
Back Dating -  
140+ firms under  
investigation,  
Brocade pays \$7M  
penalty

*The regulatory and legal environment is reaching a tipping point, shifting from the presumption of good behavior to the presumption of bad behavior. Increasingly, companies will be asked to prove authenticity of ESI.*

# Expert Testimony on Process and Controls – A Risky Strategy



*Given the permutations of controls that must work flawlessly together over a record's life cycle, opposing counsel can easily create reasonable doubt and discredit your ESI simply by attacking the controls around the evidence!*

# Forensic Analysis Isn't the Answer

## *It's Expensive*

- ▶ \$1800 per GB to process, per IDC
- ▶ Routine cases might cost \$100s of thousands simply to establish authenticity and get ESI admitted as evidence...
- ▶ ...in the hope that that your lawyers can tell a better story than the other guy's lawyers

## *It's Risky*

- ▶ Antiforensics techniques are on the rise
  - TimeStomp
- ▶ *"For any case that relies on digital forensic evidence, it would be a cakewalk to come in and blow the case up. I can take any machine and make it look guilty, or not guilty. Whatever I want ...the presumption of reliability is unjustified."*
  - Vincent Liu, partner at Stach & Liu, a forensics firm

"How Online Criminals Make Themselves Tough to Find, Near Impossible to Nab", by Scott Berinato, CSO, CIO Magazine, May 31, 2007

# Securing the Perimeter Is No Longer A Sufficient Information Security Strategy



*“The security industry has been running backwards in our view - starting at the edge (perimeter) and working its way to the actual point of the intent - the data itself...the availability and protection of the data is the core.”*

— Peter Kuper  
Morgan Stanley analyst  
March 15, 2007 research brief

*“We’re moving away from thinking about security as a perimeter issue. We need to protect the data and allow access only to those who need access. Whether the data is at rest or in motion, it needs to have adequate protection around it...we have been focused for a long time on protecting the perimeter and keeping people out. We need to transition that thinking and focus on how to collaborate and allow people to have access, whilst at the same time protecting what is most important to us - the information we have in those systems.”*

- Rhonda MacLean  
Global Chief Information Security Officer, Barclays



# Data Authenticity – An Insider Threat!

## problem 1

Security controls stop at the application layer...

- ▶ Few controls exist at the content layer itself, so integrity is inferred based on data's context and custody
- ▶ But there is no way to prove it

## problem 2

...Insiders control the controls and can do virtually anything they want to ESI...

- ▶ If one can get to the data or exert control over the controls around the data...then all bets are off.
- ▶ Every organization has people (eg, DBA, sysadmin) who have access to the data and control the controls around the data. They can do virtually anything they want, without detection. There is no way to know if data have been changed
- ▶ Even non-technical people can manipulate data - email, Acrobat, Photoshop

## problem 3

...Insiders often have economic incentives to manipulate ESI by exerting control over the controls of the data

- ▶ In the current environment, regulators often start with a presumption of bad behavior.
- ▶ So how can a trusted insider prove good behavior (prove a negative)?



# The Bar Is Being Raised To Establish the Legal Authenticity of ESI

Court declines three times to admit Amex' business records as evidence ...even though defense had no legal counsel.

- December 2005

Amex  
v  
Vee Vinhnee

Lorraine  
v  
Markel

Case Law

Federal Rules  
Of Civil  
Procedure

Federal Rules  
Of Evidence

Sedona  
Working  
Groups

*"Considering the significant costs associated with discovery...it makes little sense to go to all the bother and expense to get electronic information only to have it excluded from evidence ...counsel would be prudent to plan to authenticate records by the most rigorous standard."*

*-Judge Paul Grimm,  
May 3, 2007*

Requires the preservation of ESI and "meet and confer" process to formulate plan for managing electronic evidence

- Amended December 2006

Sedona is now laying out principles for how ESI should be managed in order to qualify as evidence...proof of authenticity is a key issue...likely to form the basis for amendments to FRE.

- Initiated May 2007

# Key Takeaways...

- ▶ If you're spending millions on preserving and producing ESI, don't neglect a strategy for proving authenticity!
- ▶ If you're put on the witness stand and asked to prove authenticity of ESI, would your controls and procedures stand up to opposing counsel?
  - What if opposing counsel has a joint J.D. - CISSP?
- ▶ If you can't quickly prove authenticity and debunk false allegations, what brand damage are you exposed to?
- ▶ Data today is constantly in motion. Given this, how can you protect data and ensure its authenticity?
  - Throwing it in a vault isn't sufficient.
  - Design for data authenticity as early in the life cycle as possible.



## Recent ESI Authenticity Cases

- No rule change yet. Rule 901 applies
- “authenticating witness [must] provide factual specificity about the process by which the electronically stored information is created, acquired, maintained, and preserved without alteration or change ...” Lorraine
- “Electronic mail communications can normally be authenticated by affidavit of a recipient, comparison of the communications content with other evidence, or statements or other statements from the purported author acknowledging the email communication.” Whatley, 2007 WL 120848 (U.S.D.C. South Carolina).
- Consider using Requests for Admission to shift costs of authentication. *But see* Hutchins 2007 WL 319990 (limiting recovery to \$40 witness fee)



## Is that E-mail an “Original” ?

- Rule 1002 requires “originals”.
- Rule 1003 permits duplicates unless there is a question as to authenticity.
- Rule 1001 says a computer “printout” is an original if it is “shown to reflect the data accurately.”



David McClellan

VP & General Manager, Financial Services

ProofSpace

Cell: 312.933.8823

[david@proofspace.com](mailto:david@proofspace.com)

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

Note: I'm free until 5 PM today to meet!

**Mark P. Henriques**

**Womble Carlyle Sandridge & Rice, PLLC**

**Phone: (704) 331-4912**

**Fax: (704) 338-7830**

**E-mail: *mhenriques@wcsr.com***

