

## e-DISCOVERY DECISIONS CONSTRUING RECENT AMENDMENT TO THE FEDERAL RULES

Phyllis Golden Morey  
National Bar Association – IP Panel Presentation  
August 1, 2007

1

## OVERVIEW

- Review of significant changes in Federal Rules
- Review of states that have passed or are considering amendments to Rules of Procedure for electronic evidence
- Litigation holds / legal holds
- E-mails: failure to preserve
- Access to Computer Hard Drives

2

## OVERVIEW (cont'd)

- Pre-December 2006 e-discovery rulings
- Post-December 2006 e-discovery rulings
  - Admonitions about discovery sanctions
  - Review of cases granting sanctions where electronic data was at issue
- Intellectual Property Rulings Pertinent to ESI
- Intellectual Property Considerations
  - Rule 26(f) Conferences
- Rule 26(f) Checklist

Q & A

3

## December 2006: Significant Changes to Federal Rules

- Rule 16F – Pretrial Conference: Discuss/Agree upon methodology for production of e-data
  - Disclosure of Electronically Stored Information (ESI) and agreements regarding assertion of privilege
- Rule 26(b)(2)(B) – Disclosure of ESI that is inaccessible
- Rule 26(b)(5)(A) – Production of ESI without waiving privilege – Claw back provisions
- Rule 26(f) – Discuss all issues pertaining to preservation of ESI
- Rule 34 – “Documents” clearly include ESI
- Rule 37 – Sanctions for failure to produce relevant ESI unless there is a “good faith” exemption

4

## State Rule Amendments that Address ESI

- The following states have addressed electronic evidence through amended rules, guidelines or protocols or are in the process of considering amendments to their procedural rules:
  - California
  - Delaware
  - Illinois
  - Kansas
  - Maryland
  - New Hampshire
  - New Jersey
  - Texas (adopted e-discovery Rules in 1999)
- Many federal courts have adopted local rules that focus specifically on Fed.R.Civ.P. 26

## I. LITIGATION HOLDS

### Issues Pertaining To Litigation Holds/Failure To Produce Complete E-Data

Trademark infringement case where plaintiff sought sanctions for defendant's failure to : (a) issue a litigation hold; (b) preserve chatroom discussions on its website; and (c) to conduct comprehensive searches for electronic records.

**RESULT:** Court denied motion for spoliation sanctions concluding

- failure to instruct all employees to preserve documents did not result in relevant documents being destroyed and
- the chatroom/instant message-type discussions were not synonymous to e-mails where more stringent discovery rules applied.

*Malletier v. Dooney & Bourke, Inc.*, 2006 WL 3851151 (S.D.N.Y. Dec. 22, 2006)

## I. LITIGATION HOLDS (cont'd)

- Trademark infringement case where Plaintiff filed motion for sanctions as a result of Defendants' routine destruction of e-mails and overriding of back-up tapes for two years while the parties exchanged letters regarding the possibility of litigation.
- Court denied motion and found no spoliation for electronic information destroyed prior to the filing of the Complaint because:
  - Letter exchanges did not include a request to preserve evidence, and
  - Letters referenced possible "exposure" but did not threaten litigation.
- However, the Court awarded monetary sanctions for Defendants' failure to adequately preserve relevant electronic records when computer hard drives were wiped clean, even though a litigation hold was in place.

*Cache Le Poudre Feeds v. Land O' Lakes Inc.*, 2007 WL 684001 (D. Col. March 2, 2007)

## II. ISSUES PERTAINING TO E-MAILS

Plaintiffs in employment termination case sought production of native file e-mails after defendants produced such e-mails in paper.

- e-mail attachments were produced in an electronic format
- e-mails were produced in a paper format
- court held that the parties negotiated during pre-trial conferences that electronic discovery would be produced as TIFF file images and not in a native file format
- plaintiff's production of e-mails in hard copy was consistent with the Rule 16 agreement – therefore motions to produce native forms of e-mails were denied

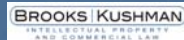
*William v. Sprint/Management Co.* 2006 WL 3691604 (D. Kan. Dec. 12, 2006)

## II. ISSUES PERTAINING TO E-MAILS (cont'd)

- Wrongful termination case - plaintiffs moved for sanctions for defendant's failure to produce and preserve relevant electronic records – e-mails, invoices, and payroll records.
- Defendant claimed no duty to supplement discovery responsive and initially claimed that it did not have the requested information.
- After the motion for sanctions was filed, defendant produced some of the requested records.

**RESULT:** Court granted sanctions - defendant's production of some documents after motion filing was evidence of bad faith. Further, defendant had the burden to prove that documents had not been destroyed since it was in control of the documents.

*May v. Pilot Travel Centers LLC*, 206 WL 3827511 (S.D. Ohio Dec. 28, 2006)



9

## II. ISSUES PERTAINING TO E-MAILS (cont'd)

- Patent infringement case where defendant filed motion to compel plaintiff to produce electronic documents because no agreement reached regarding e-discovery scope at attorney meeting before Rule 26 conference
  - Plaintiff only produced e-data for one employee
  - Defendant sought all e-documents created by every employee at plaintiff's company
  - Plaintiff response: All relevant documents produced, company-wide search unreasonable and expensive

### **RESULT:**

Court issued compromise order – electronic records/e-mails of 10 employees must be produced

*Flexsys America LP v. Kuhmo Tire USA*, 2006 WL 3526794 (N.D. Ohio 12/6/06)

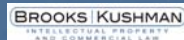


10

## II. ISSUES PERTAINING TO E-MAILS (cont'd)

- Plaintiff's sought the production of e-mail from seven of Defendant's employees as the e-mails were sent various times during the pendency of the lawsuit.
- Plaintiff argued that the defendant implemented a new e-mail deletion policy in 2003, whereby, emails were deleted within 90 days of creation, unless designated for retention.
- Plaintiff sought permission to depose defendant's employees to determine whether the defendant would be able to retrieve any of the deleted emails.
- The court examined FRCP 34 and determined that "[e]lectronic data, such as e-mails, are discoverable [and] ... that deleted emails are in most cases, not irretrievably lost."
- Therefore, the court allowed plaintiff permission to depose IT personal to determine whether any of the deleted emails could be retrieved.

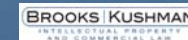
*Wells v. Xpedx*, 2007 U.S. Dist. LEXIS 29610 (M.D. Fla. April 23, 2007)



11

## II. ISSUES PERTAINING TO E-MAILS (cont'd)

- In a suit alleging violations of the Americans with Disabilities Act, the plaintiffs sought the production of backup tapes of certain electronic documents written and received after the lawsuit was filed.
- Defendant's email system automatically deleted all e-mails after 60 days and, during discovery, defendant acknowledged it did nothing to stop the automatic deletion feature.
- Defendant argued that such an order to produce backup tapes would create undue burden and expense and that there was little reason to believe that the backup tapes would produce anything of relevance.
- The court examined the FRCP advisory committee notes and considered the following factors in determining whether to order production of the backup tapes. In particular, the court stated that the committee suggests a court take into consideration the following factors:

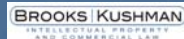


12

## II. ISSUES PERTAINING TO E-MAILS (cont'd)

- the specificity of the discovery request,
  - the quantity of information available from other and more easily accessed sources,
  - the failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources,
  - the likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources,
  - predictions as to the importance and usefulness of the further information, 6) the importance of the issues at stake in the litigation, and
  - the parties resources.
- The court found that using these factors overwhelmingly demonstrated that the production of backup tapes was warranted.

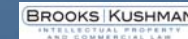
*Disability Rights Council of Greater Washington v. Washington Metropolitan Transit Auth.*, 2007 U.S. Dist LEXIS 39605 (D.D.C. June 1, 2007)



13

## III. ACCESS TO COMPUTER HARD DRIVES

- Before the December 2006 Fed. Rule Amendments, several courts allowed digital imaging of hard drive when opposing party's forensic expert was present to observe
  - U.S. Dist. Kansas – *Balboa Threadworks Inc. v. Stucky*, 2006 U.S. Dist. LEXIS 29265, 2006 WL 763668 at 4 (D. Kan. Mar. 2006)
  - E.D.N.Y. – *Fox Indus. V. Gurovich*, 2004 U.S. Dist. LEXIS 26778, 2004 WL 2348365 at 3 (E.D.N.Y. Aug. 2004)
  - E.D.Va. – *Physicians Interactive v. Lathian Sys*, 2003 U.S. Dist. LEXIS 22868, 2003 WL 23018270 at 10 (E.D. Va. Dec. 2003)
  - D. Minn. – *Antioch Co. v. Scrapbook Borders, Inc.* 210 F.R.D. 645, 652 (D. Minn. 2002)
  - S.D. Ind. – *Simon Prop. Group L.P. v. MySimon, Inc.*, 294 F.R.D. 639, 641 (S.D. Ind. 2000)



14

## III. ACCESS TO COMPUTER HARD DRIVES (cont'd)

Pre-December 2006 e-Discovery – Overview Of Court's Rationale For Rule 34(a) Access to Electronic Databases

- The pre-December 2006 courts considered the following circumstances as giving rise to a need to allow a party or a party's expert to examine the opposing party's hard drive:
  1. When a party has discrepancies or inconsistencies in discovery responses;
  2. When the defendant allegedly used a computer to commit an improper act that is the subject of the lawsuit;



15

## III. ACCESS TO COMPUTER HARD DRIVES (cont'd)

Pre-December 2006 e-Discovery – Overview Of Court's Rationale For Rule 34(a) Access To Electronic Databases

3. When trade secrets were allegedly taken and downloaded onto a computer;
4. When computers were allegedly used to disseminate plaintiff's confidential and proprietary information; and
5. When there was a NEXIS between the allegations in the complaint and computers within the possession of the opposing party.



16

### III. ACCESS TO COMPUTER HARD DRIVES (cont'd)

- Trade Secret Misappropriation, Computer Fraud and Abuse, Breach of Fiduciary Duty case where Plaintiffs' sought image of computer hard drives of home and office computers of defendants who are former employees of plaintiffs.
- Plaintiff's discovery requests sought e-mails containing specific communications relating to the claims
- Plaintiff filed motion to compel production of computer hard drives for imaging of office and home computers of employees
- Court allowed independent expert to obtain and search mirror image of defendant's computer equipment
- Amendment to 34(a) allows inspection or sampling or copying of ESI but rule does not give unfettered right of direct access to party's ESI



17

### III. ACCESS TO COMPUTER HARD DRIVES (cont'd)

- Because a relevant e-mail had not been produced during discovery, an independent expert prepared mirror image of hard drive

#### RESULT:

Court ordered defendants to produce their hard drives for imaging because the complaint contained allegations relating to this discovery request (alleged downloading of trade secrets onto computer) with computer forensics expert to be chosen by plaintiff to conduct Imaging

*Ameriwood Industries*, 2006 U.S. Dist. LEXIS 93380, 2006 WL 3825291 (E.D. Mo. 12/27/06) citing *Balboa Threadworks v. Stucky*, 2006 WL 763668 at p. 3 (D. Kan. 3/24/06) and *Physicians Interactive v. Lathian Sys. Inc.*, 2003 WL 2301827 at p. 100 (E.D. Va. 12/5/03)

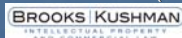


18

### III. ACCESS TO COMPUTER HARD DRIVES (cont'd)

- Trade secret misappropriate claim - Plaintiff seeks digital image of hard drive in presence of opposing party's forensic expert
- Court adopted the analysis of *Ameriwood Indus. Inc. v. Liberman* - allowed plaintiff to select a computer forensic expert who would oversee and complete the imaging of all of the defendants computer equipment. The expert follows a three-step plan borrowed from the Ameriwood case. The three-step plan included:
  - **Imaging** – The plaintiff selects computer forensics expert who will produce a mirror image of all the defendants' computers and portable hard drives.
  - **Recovery** – the expert will recover every computer document from the defendant's imaged computers and portable hard drives. The expert will provide recovered files to the defendant and notify the plaintiff that the recovery procedure is completed.
  - **Disclosure** – The defendant will then review the recovered data for privileged information and send plaintiff's counsel all non-privileged responsive documents, as well as, a log of all privileged data not sent to the plaintiff.

*Cenveo Corp. v. Slater*, 2007 U.S. Dist. LEXIS 8281 (D. Pa. Jan. 31, 2007) citing *Ameriwood Indus., Inc. v. Liberman*, 2006 U.S. Dist. LEXIS 93380 (D. Mo. 2006).



19

### III. ACCESS TO COMPUTER HARD DRIVES (cont'd)

- Case involving theft of computer equipment and unfair competition - In response to requests to produce opposing counsel hard drives for computers used by the individual defendants (former employees of the plaintiffs) for either their previous or new business ventures.

#### RESULT: The Court denied the request.

- Because the plaintiffs did not make a specific reference to information sought by inspecting the hard drives, nor did they claim that defendants failed to produce the requested information and that such information was contained on the hard drives.
- FRCP 34 allows a party to request a search of the opposing party's computers. However, most courts have found that a party is entitled to direct access to another party's databases **only** when there has been a failure to comply with the discovery rules or with specific discovery requests.

*Balfour Beatty Rail Inc. v. Vaccarello & Byers*, 2007 U.S. Dist. LEXIS 3581 (M.D. Fla. Jan. 18, 2007)

Similar holdings in *Floeter v. City of Orlando*, 2006 U.S. Dist. LEXIS 19577 (M.D. Fla. 2006) and *In re Ford Motor Co.*, 345 F.3d 1315, 1317 (11th Cir. 2003)



20

### III. ACCESS TO COMPUTER HARD DRIVES (cont'd)

- Computer Fraud and Abuse Act claim where Plaintiff sought production of laptop and personal computer hard drive for inspection. The Court noted that most Rule 34 requests for electronic data or hard drive imaging will require a balancing of the costs incurred to do the digital image against the need for the requested party to obtain this information. The Court allowed an image of the hard drive to be conducted using the following process:
  - Computer forensic expert to make images of hard drive
  - Hard drive copies to be provided to the Court and requesting parties' expert
  - Image provided to the Court and to the opposing party to assert privilege of work product for appropriate documents
- Opposing party objects to the production of any other requested files
- Forensic expert authorized to search for indication that information was provided from a different computer to the subject computer and to determine what types of memory devices were used to share the digital information.

*Frees, Inc. v. McMillian*, 2007 U.S. Dist. LEXIS 4343 (W.D. La. Jan. 22, 2007)



21

### III. ACCESS TO COMPUTER HARD DRIVES (cont'd)

- Civil claim for Computer Fraud and Abuse Act violations and breach of fiduciary duty, plaintiffs sought to inspect and obtain mirror images of the hard drives of defendants', former plaintiff employees, computers used at their new company. The parties agreed that the hard drives of the individuals defendants should be preserved, but they wanted to have their forensic expert conduct a search of the hard drives needed to satisfy plaintiff's requests.
  - The Court denied a grant of access to the hard drives concluding that plaintiff had not shown that
  - defendants had failed to produce all responsive documents requested,
  - that there had been any inconsistencies or discrepancies in the responses provided to discovery,
  - that relevant documents had been lost, thereby requiring a more exhaustive electronic search to find lost information.

*Calyon v. Mizuho Securities USA Inc.*, 2007 U.S. Dist. LEXIS 36961 at 18 (S.D.N.Y. May 18, 2007)

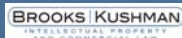


22

### III. ACCESS TO COMPUTER HARD DRIVES - CONCLUSION

#### Strategies To Be Successful In Seeking Access To Opposing Party's Computer Hard Drive

- There is greater likelihood of getting access to opposing party's hard drives if the request to image/inspect an opposing party's computer hard drive is narrowed or limited in some way to
  - the specific allegations of the Complaint or to narrowly drafted document requests, and
  - the access sought is less than "full and unfettered" searching of files
- Courts balance a request to inspect computer hard drives against claims of privilege, privacy, and confidentiality with respect to electronically stored information that is not relevant to the litigation at hand. In addition, the courts are balancing the cost and expense of imaging hard drives when claims are made that the information is inaccessible.



23

### IV. INTELLECTUAL PROPERTY RULINGS PERTINENT TO ESI

Copyright infringement lawsuit where Plaintiffs claimed Defendants received profits from online piracy of plaintiffs' copyrighted works - downloadable movies - through the operation of Defendant's internet website. Plaintiffs sought court order for the preservation and retention of IP addresses of individual users, the requests made to download the files and the dates and times such requests were made. Key factors:

- The requested information ("server log data") was only temporarily stored on the website Defendant's remote access memory (RAM).
- Plaintiffs argued that the production of the server log data was relevant to determine whether Defendant's website users have directly infringed Plaintiffs' copyrighted works and whether Defendants' website facilitate or contribute to the infringement.
- Defendants argued that the preservation and production requested would constitute a violation of several federal statutes, privacy rights and free speech rights of the IP users and would adversely impact their good will thereby causing them to lose business if they are required to produce the server log data.

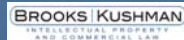


24

#### IV. INTELLECTUAL PROPERTY RULINGS PERTINENT TO ESI (cont'd)

The Magistrate Judge conducted an evidentiary hearing and made the following conclusions:

- The Server Log Data constituted Electronically Stored Information (ESI) because it was data “stored in any medium from which **information could be obtained**” and because Rule 34(a) applies to information that is “**fixed in a tangible form** and . . . is stored in a medium from which **it can be retrieved and examined.**”
- Requiring the production of the server log data was not tantamount to the creation of new data because the data was generated by the website users, it was received by the web server and it was utilized to respond to the users’ requests.
- The preservation of the server log data only would not be unduly burdensome for Defendants since the log data was a small subset of the total volume of data transmitted.
- No privacy concerns, free speech concerns or statutory violations (e.g., Stored Communications Act, Wiretap Act, or Pen Register Act) were implicated because the IP addresses of the users would be masked and other exceptions under the statutes apply to the factual circumstances here.



25

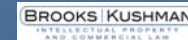
#### IV. INTELLECTUAL PROPERTY RULINGS PERTINENT TO ESI (cont'd)

The court analyzed the factors listed under FRCP 26(b)(2)(C) :

- Whether the discovery sought is cumulative or duplicative
- Whether the discovery sought can be obtained from a more convenient and less burdensome source
- Whether the party seeking the discovery had ample opportunity to obtain the information during discovery
- Whether the burden or expense of the requested discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the resources of the parties and the importance of the issues at state in the litigation.

Upon granting the order to preserve and produce the server log data that was temporarily stored in RAM, the court denied the request for sanctions concluding that the Defendant’s failure to “retain the Server Log Data in RAM was based on a good faith belief that preservation of data temporarily stored only in RAM was not legally required.” The court ordered the defendants to commence a retention policy within seven days of the hearing.

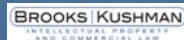
*Columbia Pictures Industries v. Justin Bunnell*, Case No. CV 06-1093, U.S. Magis. Judge ( C.D.Cal. May 29, 2007) (unpublished) (on appeal).



26

#### V. INTELLECTUAL PROPERTY CONSIDERATIONS DURING RULE 26(f) CONFERENCES

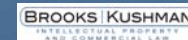
- Patent, Trademark and Copyright Infringement claims – Rule 26(f) conferences
  - Consider strategies to ensure preservation of electronically stored information (ESI) at the Rule 26(f) conference to reduce the potential for spoliation claim to be asserted
  - Anticipate your client’s claims/defenses/evidentiary needs and review checklist of items to discuss with opposing counsel that includes:
    - Record retention policies
    - Automatic destruction of e-mails/electronic files/etc.
    - Overwriting of back-up tapes
    - Timing for routine records clean-up and destruction
    - Implementation of Litigation Holds



27

#### V. INTELLECTUAL PROPERTY CONSIDERATIONS DURING RULE 26(f) CONFERENCES (cont'd)

- In patent infringement cases involving computer software, discuss location/retention of original source code and executable code, archived codes/software revisions from the original code to the current code
- Consider ESI that will impact prior art, the date of conception of invention, prior inventorship issues, etc. and discuss
  - All possible locations of ESI that describe
    - the earliest conception of the invention,
    - when the invention was reduced to practice,
    - the success/failure of the alleged prior invention,
    - metadata for the above-described information, and
    - all collections of prior art in the opposing party’s possession or about which the opposing party is aware



28

## V. INTELLECTUAL PROPERTY CONSIDERATIONS DURING RULE 26(f) CONFERENCES (cont'd)

- Whether such ESI currently exists, has been destroyed, is it on servers, desktops, laptops, home computers, back-up tapes, archives, etc.
- In copyright infringement cases, explore ESI that impacts the earliest date on which the opposing party sought permission, requested permission and received notification that permission was denied by a registrant
- Since the potential for Rule 34(a) inspections of computer hard drives or mirror images will likely be premised upon some omission or inconsistency in your opponent's discovery requests, carefully drafted discovery that explores the location, retention, and destruction of ESI should incorporate the above-described inquiries, at a minimum

## VI. RULE 26(f) CHECKLIST

Generally when preparing for the 26(b) discovery conference, the parties should consider the following comprehensive checklist of e-Discovery items to be discussed:

- The anticipated scope of requests for, and objections to, production of ESI, as well as the form of production of ESI
- Whether Meta-Data is requested for some or all ESI and, if so, the volume and costs of producing and reviewing said ESI.
- Preservation of ESI during the pendency of the lawsuit
- Post-production assertion, and preservation or waiver of, the attorney-client privilege, work product doctrine, and/or other privileges
- Identification of ESI that is or is not reasonably accessible without undue burden or cost.

## VI. RULE 26(f) CHECKLIST (cont'd)

- Methods of identifying segments of ESI produced in discovery should be discussed.
- Method and manner of redacting information from ESI if only part of the ESI is discoverable.
- Specific facts related to the costs and burdens of preservation, retrieval, and use of ESI.
- Cost sharing for the preservation, retrieval and/or production of ESI.
- Search methodologies for retrieving or reviewing ESI.
- Preliminary depositions of information systems personnel, and limits on the scope of such depositions.
- The need for two-tier or staged discovery of ESI.
- The need for any protective orders or confidentiality orders.
- Request for sampling or testing of ESI.
- Any agreement concerning retention of an agreed-upon Court expert.

# Q & A