IMLA | Miami, Florida | October 18-21, 2009



SURFING THE E-DISCOVERY TSUNAMI

An E-Discovery Surfer's Guide to Avoiding Reefs and Wipeouts in Construction and Civil Litigation

SURFING THE E-DISCOVERY TSUNAMI



Introduction

- What is E-Discovery really about?
- Why should clients care?
- Why should you care?

SURFING THE E-DISCOVERY TSUNAMI



- What is Electronically Stored Information (ESI)?
- Where is ESI located?
- Many more places than you think!

SURFING THE E-DISCOVERY TSUNAMI



- Typical office software
  Word, excel, dbase, presentation, email
- Estimating software
- Scheduling software
  Primavera, MS Project
- Project Management Software
  Expedition, Prolog, Etc
- Design software
  CAD, BIM, STAAD, Etc
- Electronic Images
- Accounting Software

TYPES OF RECORDS

- Contracts
- Drawings
- Specifications
- Meeting minutes
- Daily reports
- Timesheets
- Job cost records
- Payroll records
- Bid documents
- Invoices
- Payment applications
- Correspondence
- Schedules
- Logs
- Submittals
- Change orders
- Photographs
- RFI's
- Test reports
- Delivery tickets
- Quantity calculations
- Purchase orders

IMLA

SURFING THE E-DISCOVERY TSUNAMI



- What about document retention policies?
- Does your client have policies?
- Does your client follow the policies?
- What do you do when the client does not have document retention policies or has not followed its policies?

SURFING THE E-DISCOVERY TSUNAMI



- E-Discovery issues in pre-litigation!
- The dreaded preservation letter.
- Strategies dealing with:
  - Sending
  - Receiving
  - Responding



- Mobilizing your client to address ESI issues.

SURFING THE E-DISCOVERY TSUNAMI



- What are the obligations to preserve ESI?
- Client's obligations to preserve ESI.
- Counsel's obligations to preserve ESI.

SURFING THE E-DISCOVERY TSUNAMI



- E-Discovery Issues During Litigation!
- What kind of information (data) is sought in e-discovery and where can it be found?
- Do you really need the ESI?
- Do you really need the “native format” of a document?
- Do you really need the “meta data”?
- How should the data be collected?
- Strategies to use in conducting e-discovery.

SURFING THE E-DISCOVERY TSUNAMI



- How should clients respond to e-discovery?
- Who should be on the client's response team?
- What should counsel be reviewing?
- What are the ethical obligations imposed on counsel in reviewing ESI, discussing ESI with clients, and in preserving the attorney-client privilege in the production of ESI?

IMLA

SURFING THE E-DISCOVERY TSUNAMI



- What are the technical production issues such as file types and production specifications, review platforms and software packages to assist in performing searches?
- What kinds of software will counsel and/or their vendors and experts need to open/view various kinds of files?
- What are the issues arising out of production of documents, images and "native" files (i.e., unaltered files that are viewed using the program that was used to create them)?

SURFING THE E-DISCOVERY TSUNAMI



- What are the pitfalls of various data collection practices?
- What are the benefits and difficulties of dealing with electronic files as opposed to paper documents?

SURFING THE E-DISCOVERY TSUNAMI



- How do you select an IT Consultant?
- What are the types of consultants available to assist clients and counsel in e-discovery?
- What are the costs of the consultants?

SURFING THE E-DISCOVERY TSUNAMI



Utilizing electronic records.

- Document management software:
  - Vendors, hosts and administrators
- Organizing and accessing the records:
  - Bibliographical coding
  - Plan and manage the coding effort
    - Fields to be tracked
    - Correct field names
    - Attachments
    - Subject
  - Searching the records

SURFING THE E-DISCOVERY TSUNAMI



- What are the costs of the e-discovery process?
- Strategies to shift the costs to the other party.
- Strategies to avoid having to produce certain costly and/or burdensome ESI.

SURFING THE E-DISCOVERY TSUNAMI



- Outsourcing the review and production of ESI.
- How to manage large numbers of off-site contract attorneys performing privilege/relevance reviews.
- Ethical considerations.

SURFING THE E-DISCOVERY TSUNAMI



- What are the privilege/relevance review practices and problems?
- Strategies to handle privilege waiver issues.
- What are “clawback” and “quick peek” agreements and do they really work?
- What are the Amendments to the Federal Rules of Evidence and their impact on review and production practices?



What must be considered in a FRCP 26(f) Conference?

- *See e.g.* United States District Court for the District of Maryland - Suggested Protocol for Discovery of Electronically Stored Information ("ESI"):
  http://www.mdd.uscourts.gov/news/news/ESIProtocol.pdf
- Summary of the suggested protocol.
- Anticipated scope of requests for, and objections to, production of ESI.
- Whether production of ESI will be in the "Native File," "Static Image," or other searchable or non-searchable formats.
- Whether some documents can be produced in paper format.
- Whether meta-data is requested for some or all ESI and, if so, the volume and costs of producing and reviewing the ESI.

IMLA

SURFING THE E-DISCOVERY TSUNAMI



What must be considered in a FRCP 26(f) Conference? - Continued

- Preservation of ESI during the lawsuit and the applicability of the “safe harbor” provisions of FRCP 37.
- Post-production assertion, and preservation or waiver of, the attorney-client privilege, work product doctrine, and/or other privileges in light of “clawback,” “quick peek,” or testing or sampling procedures, and including that protocol in an order to be entered by the court.

SURFING THE E-DISCOVERY TSUNAMI



What must be considered in a FRCP 26(f) Conference? - Continued

- Identification of ESI that is or is not reasonably accessible without undue burden or cost.
- Methods of identifying ESI that is produced (file naming protocols).
- Methods of redacting information from ESI.
- Nature of the information systems used by the parties.
- 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.

SURFING THE E-DISCOVERY TSUNAMI



What must be considered in a FRCP 26(f) Conference? - Continued

- Search methodologies for retrieving or reviewing ESI.
- Preliminary depositions of information systems personnel, and the limits on the scope of such depositions.
- Whether two-tier or staged discovery of ESI needs to be conducted.
- Whether there is a need for any protective orders or confidentiality orders.

SURFING THE E-DISCOVERY TSUNAMI



FRCP 37 – Safe Harbor

- What is the safe harbor?
- Does the safe harbor really exist?
- Strategies to make it into the “harbor.”

SURFING THE E-DISCOVERY TSUNAMI



- Strategies to handle various evidentiary issues and problems with ESI.
- How do you use the ESI as evidence?
- Authentication issues.
- Hearsay Rule and exceptions.
- Best Evidence Rule.

SURFING THE E-DISCOVERY TSUNAMI



- What are the issues arising out of the creation of privilege logs?
- Strategies to deal with privilege logs.

SURFING THE E-DISCOVERY TSUNAMI



- How do you handle the problems arising out of a judge's lack of personal practical experience in actually performing e-discovery ?
- Translation - how do you tell the judge that he is wrong about an ESI issue and not be held in contempt of court!

SURFING THE E-DISCOVERY TSUNAMI



Questions

SURFING THE E-DISCOVERY TSUNAMI



Presenters:

Roy Cooper
Associate Vice President
PinnacleOne an ARCADIS company
213 Court Street
Suite 700
Middletown, CT 06457
Office: (860) 704-6100
Fax: (860) 704-6120
rcooper@pinnacleone.com

Edwin M. Levy
Senior Counsel
Commercial & Real Estate Litigation Division
New York City Law Department
100 Church Street
New York, NY 10007
Direct: (212) 788-1185
elevy@law.nyc.gov

John S. Rannestad
Senior Consultant
PinnacleOne an ARCADIS company
213 Court Street
Suite 700
Middletown, CT 06457
Office: (860) 704-6100
Fax: (860) 704-6120
jrannestad@pinnacleone.com

Donald C. Ramsay
Stinson Morrison Hecker LLP
10975 Benson, Suite 550
12 Corporate Woods
Overland Park, KS 66210
Direct: (913) 344-6744
Mobile: (913) 709-8323
Fax: (913) 344-6784
DRamsay@stinson.com

John P. Markovs
Associate County Attorney
Division of Finance and Procurement
Office of the County Attorney
Montgomery County, Maryland
101 Monroe Street, 3rd Floor
Rockville, MD 20850
Direct: (240) 777-6725
Mobile: (301) 525-3643
Fax: (240) 777-6706
john.markovs@montgomerycountymd.gov

IMLA

THE SEDONA CONFERENCE® WORKING GROUP SERIES



THE SEDONA CONFERENCE® "JUMPSTART OUTLINE": QUESTIONS TO ASK YOUR CLIENT AND YOUR ADVERSARY TO PREPARE FOR PRESERVATION, RULE 26 OBLIGATIONS, COURT CONFERENCES AND REQUESTS FOR PRODUCTION (PUBLIC COMMENT DRAFT)

A Project of The Sedona Conference®
Working Group on Electronic Document
Retention & Production (WG1)

MAY 2008 (Subject to Periodic Updating)

Copyright © 2008, The Sedona Conference®



The Sedona Conference® "Jumpstart Outline"

Copyright © 2008 The Sedona Conference®
All Rights Reserved

This outline was initially prepared by Ariana Tadler for The Sedona Conference® Institute's program entitled "Getting Ahead of the eDiscovery Curve: Strategies to Reduce Costs & Meet Judicial Expectations" held March 13-14, 2008 at The Westin Horton Plaza San Diego, San Diego, CA as an example of a tool to assist counsel in dealing with electronic discovery issues. The Sedona Conference® is seeking feedback on this outline as it is reviewed and used by practioners in real world discovery situations.

COMMENTS AND SUGGESTIONS SHOULD BE DIRECTED TO:
Ken Withers at:
The Sedona Conference®
5150 North 16th Street, Suite C 152
Phoenix, AZ 85016
(602) 258-2499 (Fax)
kwithers@sedona.net (e-mail)



Copyright © 2008
The Sedona Conference®

Visit www.thesedonaconference.org

This outline sets forth, by way of example only, a series of topics and questions to ask your client and your adversary as you prepare for meeting obligations related to preservation, Rule 26, court conferences and requests for production. The answers to these questions will guide you in (i) instructing your client about its preservation and production obligations and (ii) understanding your adversary's systems and preservation efforts to date and then structuring your discovery requests addressed to your adversary. This is a simplified outline to assist, in particular, those people who have had only limited experience in dealing with electronic discovery. As those who have had extensive experience in this arena know, the process of questioning and even the questions themselves are iterative in scope. With each answer that you elicit, inevitably additional questions must be asked. Hopefully, having an outline like this within easy reach will serve as a "jumpstart" to encourage transparency and dialogue for a successful Rule 26(f) meet and confer.

1. Document Retention Policy

1.1. Do you have a document retention (or records management) policy? Is it a written policy?

1.1.1. If yes, when was the policy implemented?

1.1.2. If yes, is the policy enforced? By whom? How?

1.1.3. If yes, did the policy change during [insert relevant time period]?

1.1.4. If yes, are you willing to produce the policy/policies?

2. Key Custodians of Potentially Relevant Information

2.1. Given the facts of the case, who are the key custodians of potentially relevant information?

2.2. To what extent has information in the possession, custody or control of the key custodians been preserved? {Discuss what those efforts have been to date and what, if any additional efforts are underway.}

2.2.1. If conferring with your client, address efforts to date and further efforts that need to be made.

2.2.2. If conferring with your adversary, discuss efforts to date and, if insufficient and appropriate, request that further efforts, as discussed, be made.

2.3. Disclosure of identities of key custodians:

2.3.1. In representing your client, consider disclosing to your adversary the identities of the key custodians for whom information has been/will be preserved.

2.3.2. If you are a requesting party, consider identifying those people who you believe are key custodians to memorialize your request for preservation of their information.

NOTE: This is an iterative process. You should plan to confer with your adversary on a recurring basis so that you can continue to update your adversary on any additional key custodians.

3. Network Servers

The questions below concern current and former database and file servers on any potentially relevant network that now store or previously stored discoverable electronic data (hereinafter referred to as "network servers"). These questions should be asked of both your client and your adversary.

3.1. Do you use, for any purpose, a network-based system? If yes, please describe.

3.2. Do you have a system that serves to back up the information managed and/or stored on the network(s)?

3.2.1. If yes, do you have at least one computer (i.e., non-incremental) backup of each of your network servers for each month for the period [insert relevant time period]?

3.2.2. If not, for which months do you/do you not have at least one complete backup?

3.2.3. For those months, if any, for which you do not have a complete backup, do you have incremental backups or other backups from which a full backup can be created of all data as of a given date in each such month?

3.2.4. If so, please describe the nature of such incremental or other backups and identify the months for which you have them.

3.3. Can specific files contained on network backups be selectively restored?

3.3.1. How? By what means?

3.3.2. Have you ever done this before?

3.3.3. In what context? Is the context such that the data restored might be deemed relevant in the context of the current litigation?

3.4. As a matter of firm policy, do you overwrite, reformat, erase, or otherwise destroy the content of the backups of your network servers on a periodic basis?

3.4.1. If so, under what circumstances?

3.4.2. If so, what is the rotation period?

3.4.3. If the rotation period has changed since [insert date], please describe the changes.

3.5. Do you maintain a company-wide intranet or other database accessible to any or some employees that provides/stores potentially relevant information? [Consider being more specific, e.g., "regarding [a particular subject]."]

3.6. Do you maintain network servers at any or all of the Company's divisions/business units/locations/offices/subsidiaries that exist separately from or in addition to Company-wide server(s)?

3.6.1. If yes, to what extent do any of those servers store any potentially relevant information in the context of this litigation?

3.6.2. Ask follow up questions consistent with the network server-based questions above.

4. Email Servers

The questions below concern the current or former servers on your network ("email servers") that now or previously stored discoverable electronic internal or external peer-to-peer messages, including email, third party email sources, and instant messages (collectively, "email").

4.1. Identify the systems (client and server-side applications) used for email and the time period for the use of each such system, including any systems used at any [overseas] facilities.

4.2. Do you maintain email servers at any or all of the Company's divisions/business units/locations/offices/subsidiaries that exist separately or in addition to the Company-wide server(s)?

4.2.1. Are the systems the same/different from those identified in Question 4.1 above? Discuss any differences.

4.3. Are end-user emails that appear in any of the following folders stored on (i) the end-user's hard-drive, (ii) an email server, or (iii) a server of a third party application service provider:

4.3.1. "In Box"?

4.3.2. "Sent Items"?

4.3.3. "Delete" or "trash" folder?

4.3.4. End user stored mail folders?

4.4. If any of your email systems have changed since [insert relevant period], identify any legacy systems, the current system(s), and the date of the last backup made with each relevant legacy system.

4.5. Do you have at least one complete (i.e., non-incremental) back up of each of your email servers for each month [for the period _____ to _____]?

4.5.1. If not, for which months do you not have at least one complete backup?

4.5.2. For those months, if any, for which you do not have a complete backup, do you have incremental or other backups from which a full backup can be created of all data as of a given date in each such month?

4.5.3. If so, please describe the nature of such incremental or other backups and identify the months for which you have them.

4.6. Does each complete email backup contain all messages sent or received since creation of the immediately prior complete email backup?

4.6.1. Do your email backups contain the messages that are in each employee's "In Box" as of the time such backup is made?

4.6.2. Do your email backups contain the messages that are in each employee's "Sent Items" folder as of the time such backup is made?

4.6.3. Do your email backups contain the messages that are in each employee's "delete" or "trash" folder as of the time such backup is made?

4.6.4. Do your email backups contain the messages that are in each employee's stored mail folders as of the time such backup is made?

4.6.5. Do your email backups contain the messages that have been stored to each employee's hard drive?

4.7. Can specific email boxes contained on email backups be restored selectively?

4.7.1. Does the Company have or maintain an index or mapping resource that would serve as a reference to identify which employees' email is stored on particular backups?

4.8. As a matter of firm policy, do you overwrite, reformat, erase, or otherwise destroy the content of the backups of your email servers on a periodic basis?

4.8.1. If so, what is the rotation period?

4.8.2. If the rotation period has changed since [insert date], describe the changes.

4.9. Did you, at any time, have a system that maintained electronic copies of all emails sent or received by certain of your employees? Do you have such a system now?

4.9.1. If so, describe the system(s) and the date(s) of first use.

4.9.2. If so, does such system(s) contain copies of all mails captured from the date of first use until the present?

4.9.3. If so, does such system(s) capture a copy of all emails sent and/or received by employees in [identify relevant departments/groups that might be relevant]?

5. Hard Drives

The questions below concern the current and former local or non-network drives contained in current or former employees' laptop and desktop computers or workstations.

5.1. As a matter of firm policy, are employees' desktop and laptop hard drives backed up in any way?

5.1.1. If so, under what circumstances?

5.1.2. If so, how long are such backups retained?

5.1.3. Please describe the backup system.

5.2. As a matter of firm policy, are employees permitted to save files, emails or other data (excluding system and application generated temporary files) to their desktop or laptop hard drives?

5.3. Since [insert relevant date], has it been technically possible for firm employees to save files, emails, or other data (excluding system and application generated temporary .files) to their desktop or laptop hard drives?

5.4. Do you implement technical impediments to minimize the opportunity for employees to save files, emails or other data (excluding system and application generated temporary files) to their desktop or laptop hard drives?

5.4.1. Is it possible for employees to override such impediments?

5.5. To what extent has a search been done to determine the extent to which any of the key custodians in this litigation did, in fact, save files, emails or other data to their desktop or laptop harddrives? Flash drives?

5.6. As a matter of firm policy, are employees' desktop and laptop hard drives erased, 'wiped," "scrubbed" or reformatted before such hard drives are, for whatever reason, abandoned, transferred or decommissioned?

5.6.1. If so, are, as a matter of fm policy, files, emails or other data stored on such hard drives copied to the respective employee's replacement drive, if any.

5.6.2. If so, as a matter of firm policy, are such files, emails or other data copied on a "bit-by-bit" basis?

6. Non-Company Computers

6.1. Does company policy permit, prohibit or otherwise address employee use of computers not owned or controlled by the company to create, receive, store or send work-related documents or communications?

6.1.1. If so, what is that policy?

6.2. Is there any technical impediment to employees using computers not owned or controlled by the company to create, receive, store or send work-related documents or communications?

Suggested Protocol for
Discovery of Electronically Stored Information ("ESI")

In light of the recent amendments to the Federal Rules of Civil Procedure regarding discovery of electronically stored information ("ESI"), a joint bar-court committee consisting of Magistrate Judge Paul W. Grimm and members of the Bar of this Court as well as technical consultants has developed a proposed protocol for use in cases where ESI may be involved. This is a working model that has not been adopted by the court but may be of assistance to counsel. It is the intent of the joint committee to review the Proposed Protocol periodically to determine if revisions would be appropriate, and after a sufficient period of time to evaluate the proposed protocol has passed, to determine whether to recommend to the Court that more formal guidelines or local rules relating to ESI be considered for adoption. To further this process, any comments and suggestions may be e-mailed to: **mdd_voyager@mdd.uscourts.gov.**

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN RE: ELECTRONICALLY STORED INFORMATION	

SUGGESTED PROTOCOL FOR DISCOVERY OF ELECTRONICALLY STORED INFORMATION

1. On December 1, 2006, amendments to Fed.R.Civ.P. 16, 26, 33, 34, 37, and 45, and Form 35, became effective, creating a comprehensive set of rules governing discovery of electronically stored information, ("ESI").

Given these rule changes, it is advisable to establish a suggested protocol regarding, and a basic format implementing, only those portions of the amendments that refer to ESI. The purpose of this Suggested Protocol for Discovery of Electronically Stored Information (the "Protocol") is to facilitate the just, speedy, and inexpensive conduct of discovery involving ESI in civil cases, and to promote, whenever possible, the resolution of disputes regarding the discovery of ESI without Court intervention.

While this Protocol is intended to provide the parties with a comprehensive framework to address and resolve a wide range of ESI issues, it is not intended to be an inflexible checklist. The Court expects that the parties will consider the nature of the claim, the amount in controversy, agreements of the parties, the relative ability of the parties to conduct discovery of ESI, and such other factors as may be relevant under the circumstances. Therefore not all aspects of this Protocol may be applicable or practical for a particular matter, and indeed, if the parties do not intend to seek discovery of ESI it may be entirely inapplicable to a particular case. The Court encourages the parties to use this Protocol in cases in which there will be discovery of ESI, and to resolve ESI

issues informally and without Court supervision whenever possible. In this regard, compliance with this Protocol may be considered by the Court in resolving discovery disputes, including whether sanctions should be awarded pursuant to Fed.R.Civ.P. 37;

SCOPE

2. This Protocol applies to the ESI provisions of Fed.R.Civ.P. 16, 26, 33, 34, or 37, and, insofar as it relates to ESI, this Protocol applies to Fed.R.Civ.P. 45 in all instances where the provisions of Fed.R.Civ.P. 45 are the same as, or substantially similar to, Fed.R.Civ.P. 16, 26, 33, 34, or 37. In such circumstances, if a Conference pursuant to Fed.R.Civ.P. 26(f) is held, it may include all parties, as well as the person or entity served with the subpoena, if said Conference has not yet been conducted. If the Conference has been conducted, upon written request of any party or the person or entity served with the subpoena, a similar conference may be conducted regarding production of ESI pursuant to the subpoena. As used herein, the words "party" or "parties" include any person or entity that is served with a subpoena pursuant to Fed.R.Civ.P. 45. Nothing contained herein modifies Fed.R.Civ.P. 45 and, specifically, the provision of Rule 45(c)(2)(B) regarding the effect of a written objection to inspection or copying of any or all of the designated materials or premises.

3. In this Protocol, the following terms have the following meanings:

A. "Meta-Data" means: (i) information embedded in a Native File that is not ordinarily viewable or printable from the application that generated, edited, or modified such Native File; and (ii) information generated automatically

by the operation of a computer or other information technology system when a Native File is created, modified, transmitted, deleted or otherwise manipulated by a user of such system. Meta-Data is a subset of ESI.

B. "Native File(s)" means ESI in the electronic format of the application in which such ESI is normally created, viewed and/or modified. Native Files are a subset of ESI.

C. "Static Image(s)" means a representation of ESI produced by converting a Native File into a standard image format capable of being viewed and printed on standard computer systems. In the absence of agreement of the parties or order of Court, a Static Image should be provided in either Tagged Image File Format (TIFF, or .TIF files) or Portable Document Format (PDF). If load files were created in the process of converting Native Files to Static Images, or if load files may be created without undue burden or cost, load files should be produced together with Static Images.

CONFERENCE OF PARTIES AND REPORT

4. The parties are encouraged to consider conducting a Conference of Parties to discuss discovery of ESI regardless of whether such a Conference is ordered by the Court. The Conference of Parties should be conducted in person whenever practicable. Within 10 calendar days thereafter, the parties may wish to file, or the Court may order them to file, a joint report regarding the results of the Conference. This process is also encouraged if applicable, in connection with a subpoena

for ESI under Fed.R.Civ.P. 45. The report may state that the parties do not desire discovery of ESI, in which event Paragraphs 4A and B are inapplicable.

A. The report should, without limitation, state in the section captioned "Disclosure or discovery of electronically stored information should be handled as follows," the following:

(1) Any areas on which the parties have reached agreement and, if any, on which the parties request Court approval of that agreement;

(2) Any areas on which the parties are in disagreement and request intervention of the Court.

B. The report should, without limitation, if it proposes a "clawback" agreement, "quick peek," or testing or sampling, specify the proposed treatment of privileged information and work product, in a manner that, if applicable, complies with the standard set forth in *Hopson v. Mayor and City Council of Baltimore*, 232 F.R.D. 228 (D.Md. 2005), and other applicable precedent. On-site inspections of ESI under Fed.R.Civ.P. 34(b) should only be permitted in circumstances where good cause and specific need have been demonstrated by the party seeking disclosure of ESI (the "Requesting Party"), or by agreement of the parties. In appropriate circumstances the Court may condition on-site inspections of ESI to be performed by independent third party experts, or set such other conditions as are agreed by the parties or deemed appropriate by the Court.

C. Unless otherwise agreed by the parties, the report described by this provision should be filed with the Court prior to the commencement of discovery of ESI.

NEED FOR PRIOR PLANNING

5. Insofar as it relates to ESI, prior planning and preparation is essential for a Conference of Parties pursuant to Fed.R.Civ.P. 16, 26(f), and this Protocol. Counsel for the Requesting Party and Counsel for the party producing, opposing, or seeking to limit disclosure of ESI ("Producing Party") bear the primary responsibility for taking the planning actions contained herein. Failure to reasonably comply with the planning requirements in good faith may be a factor considered by the Court in imposing sanctions.

EXCHANGE OF INFORMATION BEFORE RULE 26(f) CONFERENCE

6. Insofar as it relates to ESI, in order to have a meaningful Conference of Parties, it may be necessary for parties to exchange information prior to the Fed.R.Civ.P. 26(f) Conference of Parties. Parties are encouraged to take the steps described in ¶7 of this Protocol and agree on a date that is prior to the Fed.R.Civ.P. 26(f) Conference of Parties, on which agreed date they will discuss by telephone whether it is necessary or convenient to exchange information about ESI prior to the conference.

A. A reasonable request for prior exchange of information may include information relating to network design, the types of databases, database dictionaries, the access control list and security access logs and rights of individuals to access the system and specific files and applications, the ESI

document retention policy, organizational chart for information systems personnel, or the backup and systems recovery routines, including, but not limited to, tape rotation and destruction/overwrite policy.

B. An unreasonable request for a prior exchange of information should not be made.

C. A reasonable request for a prior exchange of information should not be denied.

D. To the extent practicable, the parties should, prior to the Fed.R.Civ.P. 26(f) Conference of Parties, discuss the scope of discovery of ESI, including whether the time parameters of discoverable ESI, or for subsets of ESI, may be narrower than the parameters for other discovery.

E. Prior to the Fed.R.Civ.P. 26(f) Conference of Parties, Counsel should discuss with their clients and each other who will participate in the Fed.R.Civ.P. 26(f) Conference of Parties. This discussion should specifically include whether one or more participants should have an ESI coordinator (*see* Paragraph 7.B) participate in the Conference. If one participant believes that the other should have an ESI coordinator participate, and the other disagrees, the Requesting Party should state its reasons in a writing sent to all other parties within a reasonable time before the Rule 26(f) Conference. If the Court subsequently determines that the Conference was not productive due

to the absence of an ESI coordinator, it may consider the letter in conjunction with any request for sanctions under Fed.R.Civ.P. 37.

PREPARATION FOR RULE 26(f) CONFERENCE

7. Prior to the Fed.R.Civ.P. 26(f) Conference of Parties, Counsel for the parties should:

A. Take such steps as are necessary to advise their respective clients, including, but not limited to, "key persons" with respect to the facts underlying the litigation, and information systems personnel, of the substantive principles governing the preservation of relevant or discoverable ESI while the lawsuit is pending. As a general principle to guide the discussion regarding litigation hold policies, Counsel should consider the following criteria:

(1) Scope of the "litigation hold," including:

(a) A determination of the categories of potentially discoverable information to be segregated and preserved;

(b) Discussion of the nature of issues in the case, as per Fed.R.Civ.P. 26(b)(1);

(i) Whether ESI is relevant to only some or all claims and defenses in the litigation;

(ii) Whether ESI is relevant to the subject matter involved in the action;

(c) Identification of "key persons," and likely witnesses and persons with knowledge regarding relevant events;

(d) The relevant time period for the litigation hold;

(2) Analysis of what needs to be preserved, including:

(a) The nature of specific types of ESI, including, email and attachments, word processing documents, spreadsheets, graphics and presentation documents, images, text files, hard drives, databases, instant messages, transaction logs, audio and video files, voicemail, Internet data, computer logs, text messages, or backup materials, and Native Files, and how it should be preserved:

(b) the extent to which Meta-Data, deleted data, or fragmented data, will be subject to litigation hold;

(c) paper documents that are exact duplicates of ESI;

(d) any preservation of ESI that has been deleted but not purged;

(3) Determination of where ESI subject to the litigation hold is maintained, including:

(a) format, location, structure, and accessibility of active storage, backup, and archives;

(i) servers;

(ii) computer systems, including legacy systems;

(iii) remote and third-party locations;

(iv) back-up media (for disasters) vs. back-up media for archival purposes/record retention laws;

(b) network, intranet, and shared areas (public folders, discussion databases, departmental drives, and shared network folders);

(c) desktop computers and workstations;

(d) portable media; laptops; personal computers; PDA's; paging devices; mobile telephones; and flash drives;

(e) tapes, discs, drives, cartridges and other storage media;

(f) home computers (to the extent, if any, they are used for business purposes);

(g) paper documents that represent ESI.

(4) Distribution of the notification of the litigation hold:

(a) to parties and potential witnesses;

(b) to persons with records that are potentially discoverable;

(c) to persons with control over discoverable information; including:

(i) IT personnel/director of network services;

(ii) custodian of records;

(iii) key administrative assistants;

(d) third parties (contractors and vendors who provide IT services).

(5) Instructions to be contained in a litigation hold notice, including that:

(a) there will be no deletion, modification, alteration of ESI subject to the litigation hold;

(b) the recipient should advise whether specific categories of ESI subject to the litigation hold require particular actions (*e.g.,* printing paper copies of email and attachments) or transfer into "read only" media;

(c) loading of new software that materially impacts ESI subject to the hold may occur only upon prior written approval from designated personnel;

(d) where Meta-Data, or data that has been deleted but not purged, is to be preserved, either a method to preserve such data before running compression, disk defragmentation or other computer optimization or automated maintenance programs or scripts of any kind ("File and System Maintenance Procedures"), or the termination of all File and System Maintenance Procedures during the pendency of the litigation hold in respect of Native Files subject to preservation;

(e) reasonably safeguarding and preserving all portable or removable electronic storage media containing potentially relevant ESI;

(f) maintaining hardware that has been removed from active production, if such hardware contains legacy systems with relevant ESI and there is no reasonably available alternative that preserves access to the Native Files on such hardware.

(6) Monitoring compliance with the notification of litigation hold, including:

(a) identifying contact person who will address questions regarding preservation duties;

(b) identifying personnel with responsibility to confirm that compliance requirements are met;

(c) determining whether data of "key persons" requires special handling (*e.g.*, imaging/cloning hard drives);

(d) periodic checks of logs or memoranda detailing compliance;

(e) issuance of periodic reminders that the litigation hold is still in effect.

B. Identify one or more information technology or information systems personnel to act as the ESI coordinator and discuss ESI with that person;

C. Identify those personnel who may be considered "key persons" by the events placed in issue by the lawsuit and determine their ESI practices, including those matters set forth in Paragraph 7.D, below. The term "key persons" is intended to refer to both the natural person or persons who is/are a "key person(s)" with regard to the facts that underlie the litigation, and any applicable clerical or support personnel who directly prepare, store, or modify ESI for that key person or persons, including, but not limited to, the network administrator, custodian of records or records management personnel, and an administrative assistant or personal secretary;

D. Become reasonably familiar[1] with their respective clients' current and relevant past ESI, if any, or alternatively, identify a person who can participate in the Fed.R.Civ.P. 26(f) Conference of Parties and who is familiar with at least the following:

(1) Email systems; blogs; instant messaging; Short Message Service (SMS) systems; word processing systems; spreadsheet and database systems; system history files, cache files, and cookies; graphics, animation, or document presentation systems; calendar systems; voice mail systems, including specifically, whether such systems

[1] As used herein, the term "reasonably familiar" contemplates a heightened level of familiarity with any ESI that is identified by opposing counsel pursuant to Paragraph 6 of this Protocol, however, that level of familiarity is conditioned upon the nature of the pleadings, the circumstances of the case, and the factors contained in Fed.R.Civ.P. 26(b)(2)(C).

include ESI; data files; program files; internet systems; and, intranet systems. This Protocol may include information concerning the specific version of software programs and may include information stored on electronic bulletin boards, regardless of whether they are maintained by the party, authorized by the party, or officially sponsored by the party; provided however, this Protocol extends only to the information to the extent such information is in the possession, custody, or control of such party. To the extent reasonably possible, this includes the database program used over the relevant time, its database dictionary, and the manner in which such program records transactional history in respect to deleted records.

(2) Storage systems, including whether ESI is stored on servers, individual hard drives, home computers, "laptop" or "notebook" computers, personal digital assistants, pagers, mobile telephones, or removable/portable storage devices, such as CD-Roms, DVDs, "floppy" disks, zip drives, tape drives, external hard drives, flash, thumb or "key" drives, or external service providers.

(3) Back up and archival systems, including those that are onsite, offsite, or maintained using one or more third-party vendors. This Protocol may include a reasonable inquiry into the back-up routine, application, and process and location of storage media, and requires

inquiry into whether ESI is reasonably accessible without undue burden or cost, whether it is compressed, encrypted, and the type of device on which it is recorded (*e.g.*, whether it uses sequential or random access), and whether software that is capable of rendering it into usable form without undue expense is within the client's possession, custody, or control.

(4) Obsolete or "legacy" systems containing ESI and the extent, if any, to which such ESI was copied or transferred to new or replacement systems.

(5) Current and historical website information, including any potentially relevant or discoverable statements contained on that or those site(s), as well as systems to back up, archive, store, or retain superseded, deleted, or removed web pages, and policies regarding allowing third parties' sites to archive client website data.

(6) Event data records automatically created by the operation, usage, or polling of software or hardware (such as recorded by a motor vehicle's GPS or other internal computer prior to an occurrence), if any and if applicable, in automobiles, trucks, aircraft, vessels, or other vehicles or equipment.

(7) Communication systems, if any and if applicable, such as ESI records of radio transmissions, telephones, personal digital assistants, or GPS systems.

(8) ESI erasure, modification, or recovery mechanisms, such as Meta-Data scrubbers or programs that repeatedly overwrite portions of storage media in order to preclude data recovery, and policies regarding the use of such processes and software, as well as recovery programs that can defeat scrubbing, thereby recovering deleted, but inadvertently produced ESI which, in some cases, may even include privileged information.

(9) Policies regarding records management, including the retention or destruction of ESI prior to the client receiving knowledge that a claim is reasonably anticipated.

(10) "Litigation hold" policies that are instituted when a claim is reasonably anticipated, including all such policies that have been instituted, and the date on which they were instituted.

(11) The identity of custodians of key ESI, including "key persons" and related staff members, and the information technology or information systems personnel, vendors, or subcontractors who are best able to describe the client's information technology system.

(12) The identity of vendors or subcontractors who store ESI for, or provide services or applications to, the client or a key person; the nature, amount, and a description of the ESI stored by those vendors or subcontractors; contractual or other agreements that permit the client to impose a "litigation hold" on such ESI; whether or not such a "litigation hold" has been placed on such ESI; and, if not, why not.

E. Negotiation of an agreement that outlines what steps each party will take to segregate and preserve the integrity of relevant or discoverable ESI. This agreement may provide for depositions of information system personnel on issues related to preservation, steps taken to ensure that ESI is not deleted in the ordinary course of business, steps taken to avoid alteration of discoverable ESI, and criteria regarding the operation of spam or virus filters and the destruction of filtered ESI.

TOPICS TO DISCUSS AT RULE 26(f) CONFERENCE

8. The following topics, if applicable, should be discussed at the Fed.R.Civ.P. 26(f) Conference of Parties:

A. The anticipated scope of requests for, and objections to, production of ESI, as well as the form of production of ESI and, specifically, but without limitation, whether production will be of the Native File, Static Image, or other searchable or non-searchable formats.

(1) If the parties are unable to reach agreement on the format for production, ESI should be produced to the Requesting Party as Static Images. When the Static Image is produced, the Producing Party should maintain a separate file as a Native File and, in that separate file, it should not modify the Native File in a manner that materially changes the file and the Meta-Data. After initial production in Static Images is complete, a party seeking production of Native File ESI should demonstrate particularized need for that production.

(2) The parties should discuss whether production of some or all ESI in paper format is agreeable in lieu of production in electronic format.

(3) When parties have agreed or the Court has ordered the parties to exchange all or some documents as electronic files in Native File format in connection with discovery, the parties should collect and produce said relevant files in Native File formats in a manner that preserves the integrity of the files, including, but not limited to, the contents of the file, the Meta-Data (including System Meta-Data, Substantive Meta-Data, and Embedded Meta-Data, as more fully described in Paragraph 11 of this Protocol) related to the file, and the file's creation date and time. The general process to preserve the data integrity of a file may include one or more of the following procedures: (a) duplication of responsive files in the file system (*i.e.*,

creating a forensic copy, including a bit image copy, of the file system or pertinent portion), (b) performing a routine copy of the files while preserving Meta-Data (including, but not limited to, creation date and time), and/or (c) using reasonable measures to prevent a file from being, or indicate that a file has been, modified, either intentionally or unintentionally, since the collection or production date of the files. If any party desires to redact contents of a Native File for privilege, trade secret, or other purposes (including, but not limited to, Meta-Data), then the Producing Party should indicate that the file has been redacted, and an original, unmodified file should be retained at least during the pendency of the case.

B. Whether Meta-Data is requested for some or all ESI and, if so, the volume and costs of producing and reviewing said ESI.

C Preservation of ESI during the pendency of the lawsuit, specifically, but without limitation, applicability of the "safe harbor" provision of Fed.R.Civ.P. 37, preservation of Meta-Data, preservation of deleted ESI, back up or archival ESI, ESI contained in dynamic systems[2], ESI destroyed or overwritten by the routine operation of systems, and, offsite and offline ESI (including ESI stored on home or personal computers). This discussion

[2] A "dynamic system" is a system that remains in use during the pendency of the litigation and in which ESI changes on a routine and regular basis, including the automatic deletion or overwriting of such ESI.

should include whether the parties can agree on methods of review of ESI by the responding party in a manner that does not unacceptably change Meta-Data.

(1) If Counsel are able to agree, the terms of an agreed-upon preservation order may be submitted to the Court;

(2) If Counsel are unable to agree, they should attempt to reach agreement on the manner in which each party should submit a narrowly tailored, proposed preservation order to the Court for its consideration.

D. Post-production assertion, and preservation or waiver of, the attorney-client privilege, work product doctrine, and/or other privileges in light of "clawback," "quick peek," or testing or sampling procedures, and submission of a proposed order pursuant to the holding of *Hopson v. Mayor and City Council of Baltimore*, 232 F.R.D. 228 (D.Md. 2005), and other applicable precedent. If Meta-Data is to be produced, Counsel may agree, and should discuss any agreement, that Meta-Data not be reviewed by the recipient and the terms of submission of a proposed order encompassing that agreement to the Court. Counsel should also discuss procedures under which ESI that contains privileged information or attorney work product should be immediately returned to the Producing Party if the ESI appears on its face to have been inadvertently produced or if there is prompt written notice of

inadvertent production by the Producing Party. The Producing Party should maintain unaltered copies of all such returned materials under the control of Counsel of record. This provision is procedural and return of materials pursuant to this Protocol is without prejudice to any substantive right to assert, or oppose, waiver of any protection against disclosure.

E. Identification of ESI that is or is not reasonably accessible without undue burden or cost, specifically, and without limitation, the identity of such sources and the reasons for a contention that the ESI is or is not reasonably accessible without undue burden or cost, the methods of storing and retrieving that ESI, and the anticipated costs and efforts involved in retrieving that ESI. The party asserting that ESI is not reasonably accessible without undue burden or cost should be prepared to discuss in reasonable detail, the information described in Paragraph 10 of this Protocol.

F. Because identifying information may not be placed on ESI as easily as bates-stamping paper documents, methods of identifying pages or segments of ESI produced in discovery should be discussed, and, specifically, and without limitation, the following alternatives may be considered by the parties: electronically paginating Native File ESI pursuant to a stipulated agreement that the alteration does not affect admissibility; renaming Native Files using bates-type numbering systems, *e.g.*, ABC0001, ABC0002, ABC0003, with some method of referring to unnumbered "pages" within each file; using

software that produces “hash marks” or “hash values” for each Native File; placing pagination on Static Images; or any other practicable method. The parties are encouraged to discuss the use of a digital notary for producing Native Files.

G. The method and manner of redacting information from ESI if only part of the ESI is discoverable. As set forth in Paragraph 11.D, if Meta-Data is redacted from a file, written notice of such redaction, and the scope of that redaction, should be provided.

H. The nature of information systems used by the party or person or entity served with a subpoena requesting ESI, including those systems described in Paragraph 7.D above. This Protocol may suggest that Counsel be prepared to list the types of information systems used by the client and the varying accessibility, if any, of each system. It may suggest that Counsel be prepared to identify the ESI custodians, for example, by name, title, and job responsibility. It also may suggest that, unless impracticable, Counsel be able to identify the software (including the version) used in the ordinary course of business to access the ESI, and the file formats of such ESI.

I. Specific facts related to the costs and burdens of preservation, retrieval, and use of ESI.

J. Cost sharing for the preservation, retrieval and/or production of ESI, including any discovery database, differentiating between ESI that is

reasonably accessible and ESI that is not reasonably accessible; provided however that absent a contrary showing of good cause, *e.g.*, Fed.R.Civ.P. 26(b)(2)(C), the parties should generally presume that the Producing Party bears all costs as to reasonably accessible ESI and, provided further, the parties should generally presume that there will be cost sharing or cost shifting as to ESI that is not reasonably accessible. The parties may choose to discuss the use of an Application Service Provider that is capable of establishing a central respository of ESI for all parties.

K. Search methodologies for retrieving or reviewing ESI such as identification of the systems to be searched; identification of systems that will not be searched; restrictions or limitations on the search; factors that limit the ability to search; the use of key word searches, with an agreement on the words or terms to be searched; using sampling to search rather than searching all of the records; limitations on the time frame of ESI to be searched; limitations on the fields or document types to be searched; limitations regarding whether back up, archival, legacy or deleted ESI is to be searched; the number of hours that must be expended by the searching party or person in conducting the search and compiling and reviewing ESI; and the amount of pre-production review that is reasonable for the Producing Party to undertake in light of the considerations set forth in Fed.R.Civ.P. 26(b)(2)(C).

L. Preliminary depositions of information systems personnel, and limits on the scope of such depositions. Counsel should specifically consider whether limitations on the scope of such depositions should be submitted to the Court with a proposed order that, if entered, would permit Counsel to instruct a witness not to answer questions beyond the scope of the limitation, pursuant to Fed.R.Civ.P. 30(d)(1).

M. The need for two-tier or staged discovery of ESI, considering whether ESI initially can be produced in a manner that is more cost-effective, while reserving the right to request or to oppose additional more comprehensive production in a latter stage or stages. Absent agreement or good cause shown, discovery of ESI should proceed in the following sequence: 1) after receiving requests for production of ESI, the parties should search their ESI, other than that identified as not reasonably accessible without undue burden or cost, and produce responsive ESI within the parameters of Fed.R.Civ.P. 26(b)(2)(C); 2) searches of or for ESI identified as not reasonably accessible should not be conducted until the prior step has been completed; and, 3) requests for information expected to be found in or among ESI that was identified as not reasonably accessible should be narrowly focused, with a factual basis supporting each request.

N. The need for any protective orders or confidentiality orders, in conformance with the Local Rules and substantive principles governing such orders.

O. Any request for sampling or testing of ESI; the parameters of such requests; the time, manner, scope, and place limitations that will voluntarily or by Court order be placed on such processes; the persons to be involved; and the dispute resolution mechanism, if any, agreed-upon by the parties.

P. Any agreement concerning retention of an agreed-upon Court expert, retained at the cost of the parties, to assist in the resolution of technical issues presented by ESI.

PARTICIPANTS

9. The following people:

A Should, absent good cause, participate in the Fed.R.Civ.P. 26(f) Conference of Parties: lead counsel and at least one representative of each party.

B. May participate in the Fed.R.Civ.P. 26(f) Conference of Parties: clients or representatives of clients or the entity served with a subpoena; the designated ESI coordinator for the party; forensic experts; and in-house information system personnel. Identification of an expert for use in a Fed.R.Civ.P. 26(f) Conference of Parties does not, in and of itself, identify that person as an expert whose opinions may be presented at trial within the meaning of Fed.R.Civ.P. 26(b)(4)(A, B).

C. If a party is not reasonably prepared for the Fed.R.Civ.P. 26(f) Conference of Parties in accordance with the terms of this Protocol, that factor may be

used to support a motion for sanctions by the opposing party for the costs incurred in connection with that Conference.

REASONABLY ACCESSIBLE

10. No party should object to the discovery of ESI pursuant to Fed.R.Civ.P. 26(b)(2)(B) on the basis that it is not reasonably accessible because of undue burden or cost unless the objection has been stated with particularity, and not in conclusory or boilerplate language. Wherever the term "reasonably accessible" is used in this Protocol, the party asserting that ESI is not reasonably accessible should be prepared to specify facts that support its contention.

PRINCIPLES RE: META-DATA

11. The production of Meta-Data apart from its Native File may impose substantial costs, either in the extraction of such Meta-Data from the Native Files, or in its review for purposes of redacting non-discoverable information contained in such Meta-Data. The persons involved in the discovery process are expected to be cognizant of those costs in light of the various factors established in Fed.R.Civ.P. 26(b)(2)(C). The following principles should be utilized in determining whether Meta-Data may be discovered:

A. Meta-Data is part of ESI. Such Meta-Data, however, may not be relevant to the issues presented or, if relevant, not be reasonably subject to discovery given the Rule 26(b)(2)(C) cost-benefit factors. Therefore, it may be subject to cost-shifting under Fed.R.Civ.P. 26(b)(2)(C).

B. Meta-Data may generally be viewed as either System Meta-Data, Substantive Meta-Data, or Embedded Meta-Data. System Meta-Data is data that is

automatically generated by a computer system. For example, System Meta-Data often includes information such as the author, date and time of creation, and the date a document was modified. Substantive Meta-Data is data that reflects the substantive changes made to the document by the user. For example, it may include the text of actual changes to a document. While no generalization is universally applicable, System Meta-Data is less likely to involve issues of work product and/or privilege.

C. Except as otherwise provided in sub-paragraph E, below, Meta-Data, especially substantive Meta-Data, need not be routinely produced, except upon agreement of the requesting and producing litigants, or upon a showing of good cause in a motion filed by the Requesting Party in accordance with the procedures set forth in the Local Rules of this Court. Consideration should be given to the production of System Meta-Data and its production is encouraged in instances where it will not unnecessarily or unreasonably increase costs or burdens. As set forth above, upon agreement of the parties, the Court will consider entry of an order approving an agreement that a party may produce Meta-Data in Native Files upon the representation of the recipient that the recipient will neither access nor review such data. This Protocol does not address the substantive issue of the duty to preserve such Meta-Data, the authenticity of such Meta-Data, or its admissibility into evidence or use in the course of depositions or other discovery.

D. If a Producing Party produces ESI without some or all of the Meta-Data that was contained in the ESI, the Producing Party should inform all other parties of this fact, in writing, at or before the time of production.

E. Some Native Files contain, in addition to Substantive Meta-Data and/or System Meta-Data, Embedded Meta-Data, which for purposes of this Protocol, means the text, numbers, content, data, or other information that is directly or indirectly inputted into a Native File by a user and which is not typically visible to the user viewing the output display of the Native File on screen or as a print out. Examples of Embedded Meta-Data include, but are not limited to, spreadsheet formulas (which display as the result of the formula operation), hidden columns, externally or internally linked files (*e.g.*, sound files in Powerpoint presentations), references to external files and content (*e.g.*, hyperlinks to HTML files or URLs), references and fields (*e.g.*, the field codes for an auto-numbered document), and certain database information if the data is part of a database (*e.g.*, a date field in a database will display as a formatted date, but its actual value is typically a long integer). Subject to the other provisions of this Protocol related to the costs and benefits of preserving and producing Meta-Data (see generally Paragraph 8), subject to potential redaction of Substantive Meta-Data, and subject to reducing the scope of production of Embedded Meta-Data, Embedded Meta-Data is generally discoverable and in appropriate cases, *see*

Fed.R.Civ.P. 26(b)(2)(C), should be produced as a matter of course. If the parties determine to produce Embedded Meta-Data, either in connection with a Native File production or in connection with Static Image production in lieu of Native File production, the parties should normally discuss and agree on use of appropriate tools and methods to remove other Meta-Data, but preserve the Embedded Meta-Data, prior to such production.

Processing - Metrics

Processing

- Processing - Overview
- Scoping Electronic Discovery Projects
- Processing Stages
  - Tape Restoration
  - File/Document Extraction
  - Metadata
  - Chain of Custody at a File Level
  - Deduplication
  - Data Culling
- Data Conversion
- Quality Control
- Reporting
- Requesting and Negotiating
- Evaluating What Has Been Received
- Audit and Chain of Custody
  - Practices to Consider
  - Copying, Fingerprinting and Analyzing Original Data
- Culling, Prioritizing and Triage
  - Understanding Background to Set Priorities
  - Planning
  - File Analysis
  - Review Team Factors
  - Using Key Words for Prioritization
- Searching
  - Search Techniques
  - Culling and Searching Considerations
- Cost Drivers
- **Metrics**
  - Means of Measuring
  - Industry Benchmark Survey
  - Paper-to-Electronic Estimate Conversion Table
- Additional Materials
- Participants

One of the biggest challenges that occurs when dealing with electronic data, is estimating the volume when all that is known is the total GB to process. Since the overall volume will have significant impact on the project as a whole, it is important to understand the circumstances that will drive that estimate.

Contents

[hide]

1 Means of Measuring
- 1.1 Pages
- 1.2 Number of Documents
- 1.3 Culling Rate
- 1.4 Non-Printable Files

2 Industry Benchmark Survey

3 Paper-to-Electronic Estimate Conversion Table

4 Footnotes

Means of Measuring

Pages

In a lot of cases the overall review time and cost for a project can be determined by the total number of pages that will be reviewed, and eventually produced. This can be better estimated the more you know about the collection. If you can separate the total volume, and identify the amount of email data, application data, and non printable data, you can get a more accurate estimate then you would base on volume alone.

Number of Documents

Since another important driver in how much effort will need to be put in to the document review, is the number of documents that will be reviewed, estimating this can be a valuable statistic. Although there are quick ways to identify the number of documents in the collection, it becomes more challenging to quickly identify the documents that will be removed from the culling process.

Culling Rate

The amount of deduplication can vary greatly based on the nature of the data (backups, live data, or a combination), the scope of the deduplication (within or across custodian), and the custodian retention habits.

Searching/Filtering is another aspect that is important to consider when estimating the overall volume that will be delivered for review. Depending on the on the number of terms, and the nature of the documents the results can vary greatly.

Non-Printable Files

Non-printable files are documents that in general will not be delivered or reviewed. Therefore it is important to exclude them from the document/GB/page estimates in order to yield more accurate results.

(**back to top**)

Industry Benchmark Survey

The table below lists some industry averages that can be used as a tool for guidance for estimating a document collection:

Benchmark	**Value**		
	High	**Median**	**Low**
Images[1] per GB	78,671	47,213	18,534
Images per file email	11	4	2
Images per file app files	63	10	3
Files per GB email	36,530	22,572	9,934
Files per GB app files	20,305	15,791	7,553
GB per custodian email	5	2	1
GB per custodian app files	4	1	0
Culling Rate Percentages			
Deduplication	51%	21%	6%
Searching/Filtering	64%	61%	23%
Non-printable files	22%	5%	2%
Processing Speeds			

Process time per GB native	117	33	11
Process time per GB image	35	32	23
Process time to first deliverable	53	35	21
Process time by file type	4	3	2
Process time by file type	6	4	3
Process time by file type	2	3	2
Quality			
First pass quality yield %[2]	57%	78%	73%

(**back to top**)

Paper-to-Electronic Estimate Conversion Table

Boxes of Documents	**Approximate Total Pages**	**Megabytes, Gigabytes, Terabytes**	
1	2,500	50	Megabytes
10	25,000	500	Megabytes
20	50,000	1	Gigabyte
100	250,000	5	Gigabyte
200	500,000	10	Gigabyte
300	750,000	15	Gigabyte
400	1,000,000	20	Gigabyte
500	1,250,000	25	Gigabyte

1,000	2,500,000	50	Gigabyte
2,000	5,000,000	100	Gigabyte
5,000	12,500,000	250	Gigabyte
10,000	25,000,000	500	Gigabyte
20,000	50,000,000	1	Terabyte
40,000	100,000,000	2	Terabyte
60,000	150,000,000	3	Terabyte

(**back to top**)

Footnotes

1. ^ Images are counted one per page, so that a 4-page multi-page TIFF would count as 4 images.
2. ^ The percentage of data that runs through without intervention or exception handling.

(**back to top**)

Category: Processing

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

Louis H. Hopson, et al.	.	
Plaintiffs,	.	
v.	.	**Civil Action No. AMD-04-3842**
The Mayor and City Council of Baltimore, A Municipal Corporation of the State of Maryland, and the Baltimore City Police Department	.	
Defendants.	.	

.....

MEMORANDUM AND ORDER

This case has been referred to me for resolution of all discovery disputes. Paper no. 27. Pending and ripe for a decision is the Plaintiffs' motion to compel Rule 33 and 34 discovery. Papers No. 26, 29, and 30. Plaintiffs have asserted putative class claims and individual claims against the City of Baltimore ("The City") and the Baltimore City Police Department ("BCPD") alleging that BCPD engaged in racial discrimination against African American police officers in connection with the administration of the disciplinary system for Baltimore police officers. It is alleged that the disparate impact and disparate treatment claims extend back to 1992, the commencement date for the misconduct that is the focus of the class claims.

When the court issued its scheduling order and discovery commenced, Plaintiffs promptly served interrogatories and document production requests on the Defendants. The Rule 34 requests were extensive and clearly sought both "hard copy" records as well as electronically stored records and data. Companion interrogatories included more than 15 specifically designed to discover the nature, extent, and location of electronically stored records, the Defendants' IT

capabilities, the nature of archived data, e-mail, and records retention policies – in short, all of the computer generated information that is the subject of so much discussion these days.

Defendants answered, raising many objections to the discovery sought, including burdensomeness and expense. Many of their objections, however, were boilerplate, general objections, rather than specific ones, as required by Fed. R. Civ. P. Rule 33(b)(4) and Rule 34. *See Hall v. Sullivan*, __ F.R.D. __, 2005 WL 2621903 (D. Md. Oct. 11, 2005). Plaintiffs and Defendants met and corresponded in an unsuccessful attempt to resolve the discovery disputes without involving the court. Plaintiffs then followed the procedures outlined in Local Rule 104.8, the issues were fully briefed and, when last efforts to work out their differences failed, the motion and responsive memoranda were filed. To support their objections based on burden and expense, which largely had been unparticularized in their initial written responses, Defendants attached the affidavit of the BCPD's IT manager, Mr. Michael Roosa. Paper No. 30, Attachment A. Although this affidavit was a welcome addition to the prior conclusory assertions of burden, and did demonstrate the limited number of IT specialists working for the BCPD and the many competing demands for their services, it still fell short of what would be necessary for a proper application of the cost-benefit analysis required by Rule 26(b)(2) to enable the court fairly to tailor the discovery allowed in this particular case. Absent, for example, was any estimate of the number of hours and or costs that would have to be expended in order to comply with the Plaintiffs' discovery requests.

On November 9, 2005, a hearing was held in open court. One of the Defendants' concerns was the cost and burden of performing pre-production privilege review of the records sought by the Plaintiffs. I ruled on many of the Rule 34 requests, and also ordered the parties to

pursue through other methods, discovery into the Defendants' electronically stored information. Specifically, because the parties had not met in an effort to agree upon a reasonable discovery plan for electronic discovery, I ordered Defendants, along with Mr. Roosa, to meet with Plaintiffs and their IT representative to consult in good faith in an effort to informally discover sufficient information about the Defendants' IT systems and electronic records to agree upon a proposed discovery plan to submit to the court for review and approval. I further ordered the parties to discuss the Rule 26(b)(2) factors in connection with the procedures that Defendants reasonably should take to perform a review for privilege and work product claims, given the nature of the litigation, the long time period for which the records were sought, and the resources of the parties. I ordered this conference to take place within 30 days, after which a follow-up hearing would be scheduled, during which I would approve a discovery plan and issue an order implementing it.

During the November 9th hearing, I noted that the issues presented in this case prominently showcase challenges that recur in connection with the discovery of electronic data, which are the subject of the proposed amendments to the Federal Rules of Civil Procedure that were approved in September 2005 by the Judicial Conference of the United States and forwarded to the United States Supreme Court for adoption, and referral to Congress for its approval. Specifically, this case highlights significant unresolved issues relating to the nature of privilege review that must be performed by a party producing electronically stored information, whether non-waiver agreements entered into by counsel to permit post-production assertion of privilege are permissible, and effective for their intended purpose, as well as the application of principles of substantive evidence law related to the waiver of privilege by inadvertent production. These

issues, among the most talked about by lawyers, judges, and the parties who are affected by their resolution, have yet to be fully developed by the courts. And, in this regard, there is no controlling precedent in the Fourth Circuit or this District to guide counsel and clients in this important and potentially hazardous aspect of discovery. I explained to counsel that I intended to supplement my oral ruling with a memorandum and order addressing these issues. This memorandum does so.

This case vividly illustrates one of the most challenging aspects of discovery of electronically stored information – how properly to conduct Rule 34 discovery within a reasonable pretrial schedule, while concomitantly insuring that requesting parties receive appropriate discovery, and that producing parties are not subjected to production timetables that create unreasonable burden, expense, and risk of waiver of attorney-client privilege and work product protection. In the absence of procedural rules tailored to ameliorate this problem, parties and courts have begun to adopt[1] innovative methods of addressing it. As noted in the Federal Judicial Center Manual for Complex Litigation:

> A responding party's screening of vast quantities of unorganized computer data for privilege prior to production can be particularly onerous in those jurisdictions in which inadvertent production of privileged data may constitute a waiver of privilege as to a particular item of information, items related to the relevant issue, or the entire data collection. Fear of the consequences of inadvertent waiver may add cost and delay to the discovery process for all parties. Thus, judges often encourage counsel to stipulate at the outset of discovery to a "nonwaiver" agreement, which they can adopt as a case-management order. Such agreements

[1] "It has become increasingly common to see parties enter into agreements to disclose privileged materials provided the disclosure is not taken to entail waiver as to all privileged matters. Because courts will give effect to such agreements, the parties by contract, so to speak, can avoid the general rule that partial disclosure on a given subject mater will bring in its wake total disclosure." Edna Selan Epstein, *The Attorney-Client Privilege and the Work-Product Doctrine*, 287-88 (4th ed. 2001).

> protect responding parties from the most dire consequences of inadvertent waiver by allowing them to "take back" inadvertently produced privileged materials if discovered within a reasonable period, perhaps thirty days from production.[2]

Similarly, the recent report of the Judicial Conference Committee on Rules of Practice and Procedure to the Chief Justice of the United States and the Members of the Judicial Conference of the United States that forwarded proposed revisions to Federal Rules of Civil Procedure 16, 26, 33, 34, and 37, addresses this same issue:

> The problems that can result from efforts to guard against privilege waiver often become more acute when discovery of electronically stored information is sought. The volume of the information and the forms in which it is stored make privilege determinations more difficult and privilege review correspondingly more expensive and time-consuming, yet less likely to detect all privileged information. Inadvertent production is increasingly likely to occur. Because the failure to screen out even one privileged item may result in an argument that there has been a waiver as to all other privileged materials related to the same subject matter, early attention to this problem is more important as electronic discovery becomes more common. Under the proposed amendments to Rules 26(f) and 16, if the parties are able to reach an agreement to adopt protocols for asserting privilege and work-product protection claims that will facilitate discovery that is faster and at lower cost, they may ask the court to include such arrangements in a case-management or other order.[3]

The commentary to the proposed changes to Rules 16(b) and 26(f) similarly states:

> Rule 16(b) is also amended to include among the topics that may be addressed in the scheduling order any agreements that the parties reach to facilitate discovery by minimizing the risk of waiver of privilege or work-product protection. Rule 26(f) is amended to add to the discovery plan the parties' proposal for the court to enter a case management or other order adopting such an agreement. The parties

---

[2] *Manual for Complex Litigation*, § 11.446, at 80, (Stanley Marcus, et al. eds., Federal Judicial Center 4th ed. 2004).

[3] *Report to the Standing Committee on Rules of Practice and Procedure, Judicial Conference of the United States by the Advisory Committee on the Federal Rules of Civil Procedure*, September 2005 at 27. In September, 2005, the Judicial Conference of the United States approved the proposed changes for submission to the Supreme Court, and recommended their adoption and that they be submitted to Congress for approval.

> may agree to various arrangements. For example, they may agree to initial provision of requested materials without waiver of privilege or protection to enable the party seeking production to designate the materials desired or protection for actual production, with the privilege review of only those materials to follow. Alternatively, they may agree that if privileged or protected information is inadvertently produced, the producing party may by timely notice assert the privilege or protection and obtain return of the materials without waiver. Other arrangements are possible. In most circumstances, a party who receives information under such an arrangement cannot assert that production of the information waived a claim of privilege or of protection as trial-preparation material.[4]

In addition, the proposed changes to Rule 26(b)(5) would allow a party to raise post-production claims of privilege and work product protection for electronically stored information, and further establish a procedure for resolving disputes regarding such an assertion. The commentary for this proposed rule change again notes the longstanding complaint that the delay and expense associated with privilege review for electronic records is excessive.[5] The proposed rule changes appear to be ideal, were it not for the following cautionary language in the comment:

> The proposed amendment does not address the substantive questions whether privilege or work product protection has been waived or forfeited [by the procedures in the proposed amendment to Rule 26(b)(5)]. Instead, the amendment sets up a procedure to allow the responding party to assert a claim of privilege or of work-product protection after production. . . . It is a nod to the pressures of litigating with the amount and nature of electronically stored information available in the present age, a procedural device for addressing the increasingly costly and time-consuming efforts to reduce the number of inevitable blunders . . . [Proposed] Rule 26(b)(5)(2) does not address whether the privilege or protection that is asserted after production was waived by the production. The courts have developed principles to determine whether, and under what

---

[4] *Report to the Standing Committee on Rules of Practice and Procedure, Judicial Conference of the United States by the Advisory Committee on the Federal Rules of Civil Procedure*, September 2005 at 26.

[5] *Id.* at 52.

circumstances, waiver results from inadvertent production of privileged or protected information.[6]

Thus, after nearly ten years of extensive study[7] of the discovery rules by the Advisory Committee on the Federal Rules of Civil Procedure, the procedures proposed to address the burdens of privilege review associated with production of electronically stored information surely would ameliorate them, but at the price of risking waiver or forfeiture of privilege/work product protection,[8] depending on the substantive law of the jurisdiction in which the litigation was pending. Absent a definitive ruling on the waiver issue, no prudent party would agree to follow the procedures recommended in the proposed rule. And, as already noted, parties, with the apparent encouragement of courts,[9] have been using these procedures even in advance of the

---

[6] *Id.* at 52, 56.

[7] *Id.* at 52.

[8] Although it is customary during Rule 34 discovery to assert simultaneously attorney-client privilege and work product protection, the two doctrines are distinct, and what is required to effect a waiver of the attorney-client privilege is not the same for waiver of work product protection. In fact, the attorney-client privilege may be waived more easily than work product protection. *See Nutramax Laboratories, Inc. v. Twin Laboratories, Inc.*, 183 F.R.D. 458, 463-64 (D. Md. 1998); *In re Martin Marietta Corp.*, 856 F.2d 619, 623-24 (4th Cir. 1988).

For purposes of this case, it is not necessary to distinguish what is needed to effect a waiver of the attorney-client privilege from waiver of work product protection. Since attorney client protection is waived more easily than work product protection, procedures that protect against waiver of the former will, *a fortiori*, prevent against waiver of the latter.

[9] *Zubulake v. UBS Warburg LLC*, 216 F.R.D. 280, 290 (S.D.N.Y. 2003) ("Indeed, many parties to document-intensive litigation enter into so-called "claw-back" agreements that allow the parties to forego privilege review altogether in favor of an agreement to return inadvertently produced privileged documents. The parties here can still reach such an agreement with respect to the remaining seventy-two tapes and thereby avoid any cost of reviewing these tapes for privilege"); *See also* The Sedona Conference, *The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production*, March, 2003, comment 10a, http://www.thesedonaconference.org (recommending that parties enter into non-waiver agreements to facilitate production of electronic records and that they seek court orders providing that such agreements do not constitute inadvertent waiver of privilege/work product.

adoption of rule changes authorizing them.

Within the Fourth Circuit, however, no case has been found that would provide definitive guidance to practitioners and their clients whether the procedures proposed by the recommended changes to the discovery rules and apparently being utilized at present by counsel, would waive attorney-client privilege or work product protection. As will be seen, forecasting the answer to this important question is not as easy as might be desired.

The changes recommended to Rules 16 and 26 encourage the party receiving the electronic discovery to agree not to assert waiver of privilege/work product protection against an opposing party that agrees to provide expedited production of electronically stored information without first doing a full-fledged privilege review. Similar agreements have been approved by a number of courts in the past. *See Zubulake*, 216 F.R.D. at 290 (see quote at n. 9); *VLT Corp. v. Unitrode Corp.*, 194 F.R.D. 8 (D. Mass. 2000) (District court approved stipulation between counsel governing non-waiver of inadvertently produced privileged documents); *Ames v. Black Entm't Television*, No. 98CIV0226, 1998 WL 812051, at *1 (S.D.N.Y. Nov. 18, 1998). ("Lee did not waive [the attorney-client] privilege, even though she answered certain questions about Ebron's alleged affair, because the parties agreed at her deposition that she could answer

---

The Sedona Conference identifies itself as a non-profit charitable research and education organization whose mission is facilitate education regarding "cutting edge issues" in law related topics including complex litigation. It has published recommended practices regarding electronic document production that have received widespread attention); *American Bar Association Civil Discovery Standards 31a.xiii*, amend. August 2004 (recommending that the parties participate in an initial discovery conference and recommends that at the conference they stipulate "to the entry of a court order providing that production to other parties or review by a mutually-agreed independent information technology consultant of attorney-client privileged or attorney work-product protected electronic data will not effect a waiver of privilege or work product protection").

selected questions and those answers would not be deemed a waiver of any privileges."); *Dowd v. Calabrese*, 101 F.R.D. 427, 439 (D.D.C. 1984) ("Plaintiffs' waiver theory fails for yet another reason. Counsel for the parties stipulated in the course of the O'Donnell deposition that testimony by the witness would not be deemed to constitute any waiver of the attorney-client or work product privileges. In view of that stipulation, plaintiffs cannot now rely on the O'Donnell deposition to support a claim of waiver."); *W'ern. Fuels Ass'n., Inc. v. Burlington N'ern. R.R. Co.*, 102 F.R.D. 201, 204 (D. Wyo. 1984) ("The Order of Magistrate Beaman dated April 18, 1983 states that, in order to expedite discovery herein, inadvertent production of privileged documents during the course of discovery herein shall not constitute a waiver of either the attorney-client privilege or the work product privilege. To the extent plaintiff alleges defendant waived such privileges through the production of documents during the course of discovery herein, the Court believes such prior order prevents a waiver."); *Eutectic Corp. v. Metco*, 61 F.R.D. 35, 42 (E.D.N.Y. 1973) ("Prior to any discovery in this case by defendant, plaintiffs and defendant executed a protective order which contemplated a special method of discovery for the particular case and expressly provided there would be no waiver of any privilege unless expressed in writing . . . . If the language of the protective order is to be applied in the instant case, its requirement of express waiver would seem to preclude any argument of waiver to be implied by a particular course of conduct especially one contemplated in the order itself."); *United States v. United Shoe Mach. Corp.* 89 F. Supp. 357, 359 (D. Mass. 1950) ("The defendant seasonably claimed whatever privilege it had. It did not waive its privilege by surrendering the exhibits in response to subpoenas, because it was agreed in advance by Government counsel that compliance with the subpoenas should not constitute a waiver."). *See also* Epstein, *supra*, at

287-88 ("It has become increasingly common to see parties enter into agreements to disclose privileged materials provided the disclosures are not taken to entail waiver as to all privileged matters. Because courts will give effect to such agreements, the parties by contract, so to speak, can avoid the general rule that partial disclosure on a given subject matter will bring in its wake total disclosure.").[10]

Although the use of "non-waiver" agreements presently may be growing - - and if the proposed changes to the discovery rules are adopted they can be expected to increase significantly - - they certainly are not risk-free. Some commentators appear to be openly skeptical of their ability to insulate the parties from waiver,[11] and even if they are enforceable as between the parties that enter into them, it is questionable whether they are effective against third-parties.[12] *See Westinghouse Elec. Corp. v. Republic of the Philippines,* 951 F.2d 1414, 1426-27 (3d Cir. 1991) (Agreement between litigant and DOJ that documents produced in response to investigation would not waive privilege does not preserve privilege against different entity in unrelated civil proceeding); *Bowne v. AmBase Corp*., 150 F.R.D. 465, 478-79 (S.D.N.Y.

---

[10] Not all courts have approved non-waiver agreements between counsel. *See Koch Materials Co. v. Shore Slurry Seal Inc*., 208 F.R.D. 109, 118 (D.N.J. 2002) (Court declined to give effect to agreement between counsel that production of certain documents would not waive privilege protection because such agreements "could lead to sloppy attorney review and improper disclosure which could jeopardize clients' cases."); *Columbia/HCA Healthcare Corp*., 192 F.R.D. 575, 577-78 (M.D. Tenn. 2000) (holding that an agreement with the government to produce documents without waiving privilege/work product protection is invalid, rejecting the doctrine of "selective waiver").

[11] 24 Charles Alan Wright & Kenneth W. Graham, *Federal Rules of Evidence,* Ch. 6 § 5507, 579 and 579 n. 22 (1986).

[12] *Id.* at 579 ("A stipulated non-waiver may be defensible as between the two parties inasmuch as they are free to argue between themselves that certain evidence will not be used. But it is questionable whether such agreements should be effective as against third parties.")

1993) (non-waiver agreement between producing party in one case not applicable to third party in another civil case).

The commentary to the proposed changes to Rule 26(b)(5) anticipates arguments that production of privileged/protected information under a non-waiver agreement will waive the privilege or protection, but asserts that "courts have developed principles for determining whether waiver results from inadvertent production of privileged information."[13] However, because there is no uniform position taken by the courts on whether inadvertent production waives privilege/work product protection, care must be taken to identify the controlling law in each jurisdiction. Specifically, three distinct positions have been taken by the courts: the "strict accountability" approach followed by the Federal Circuit and the First Circuit[14] (which almost always finds waiver, even if production was inadvertent, because "once confidentiality is lost, it can never be restored");[15] the lenient/ "to err is human" approach, followed by the Eighth Circuit and a handful of district courts[16] (which views waiver as requiring intentional and knowing relinquishment of the privilege, and finds waiver in circumstances of inadvertent disclosure only

---

[13] Comment to proposed changes to Rule 26(b)(5) at 15. *See also* comment to proposed changes to Rule 16(b) at 3 ("Alternatively, [the parties] . . . may agree that if privileged information is inadvertently produced the producing party may by timely notice assert the privilege and obtain return of the materials without waiving the privilege."); Manual for Complex Litigation, *supra*, § 11.446 (Non-waiver agreements "protect responding parties from the most dire consequences of inadvertent waiver by allowing them to 'take back' inadvertently produced privileged materiels if discovered within a reasonable period, perhaps thirty days from production.").

[14] Epstein, *supra*, at 309.

[15] *Id.* The District of Columbia Circuit also adheres to the strict liability approach. Saltzburg et al, *Federal Rules of Evidences Manual*, §501.02[5][k][v] at 501-54 (8th ed. 2002); *citing In re Sealed Case*, 877 F.2d 976 (D.C. Cir. 1989).

[16] Epstein, *supra*, at 310-11.

if caused by gross negligence);[17] and the third approach, adopting a "'balancing' test that requires the court to make a case-by-case determination of whether the conduct is excusable so that it does not entail a necessary waiver."[18]

The Fourth Circuit has not yet considered the doctrine of inadvertent disclosure of attorney client/work-product materials in the context of voluminous production during discovery in a civil case.[19] However, its discussion of the doctrine of waiver in other contexts provides useful circumstantial evidence of how they might rule.

In *In re Grand Jury Proceedings*, 727 F.2d 1352 (4th Cir. 1984) the Fourth Circuit examined the attorney-client privilege and its waiver in the context of a subpoena issued to a lawyer to testify before a grand jury regarding a client's business activities. The court narrowly interpreted the privilege because its application "'impedes [the] full and free discovery of the truth' and is 'in derogation of the public's right to every man's evidence,'" accordingly the court stated that it "is to be 'strictly confined within the narrowest possible limits consistent with its principle.'"[20] The court noted that "the essence of the privilege is that the communication was

---

[17] *Id.*

[18] *Id.* at 311. A number of district courts within the Fourth Circuit have adopted this approach. *See F.C. Cycles Inc. v. FILA*, 184 F.R.D. 64, 76 (D. Md. 1998) ("Of late, however, numerous district courts in this circuit have embraced the balancing test [regarding waiver of attorney-client privilege for inadvertently disclosed material]")*; see also McCafferty's v. The Bank of Glen Burnie*, 179 F.R.D. 163, 167-69. (D. Md. 1998) *citing In re Grand Jury Proceedings*, 142 F.R.D. 276, 279 (M.D.N.C. 1992); *F.D.I.C. v. Marine Midland Realty Credit Corp.*, 138 F.R.D. 479 (E.D. Va. 1991).

[19] *F.C. Cycles Int'l, Inc.*, 184 F.R.D. at 76.

[20] *In re Grand Jury Proceedings*, 727 F. 2d at 1355 (internal citations omitted).

intended to be confidential"[21] adding: "In fact, so strong is this requirement of confidentiality that it has been held that the privilege may be lost 'even if the disclosure is inadvertent' such as in some circumstances 'eavesdropping' and again, where if the privileged communication consisted of 'privileged documents,' the party did not 'take reasonable steps to insure and maintain [their] confidentiality.'"[22] The court continued: "It is not asking too much to insist that if a client wishes to preserve the [attorney client] privilege . . . he must take some affirmative action to preserve confidentiality . . . [t]aking or failing to take precautions may be considered as bearing on intent to preserve confidentiality. In particular, courts have consistently 'refused to apply the privilege to information that the client intends his attorney to impart to others . . . .'"[23] Finally, the court stated that "[a]ny disclosure inconsistent with maintaining the confidential nature of the attorney-client relationship waives the attorney-client privilege. Any voluntary disclosure by the client to a third-party waives the privilege not only as to the specific communication disclosed, but often as to all other communications relating to the same subject matter."[24] Although one respected commentator has cited *In re Grand Jury Proceedings* for the proposition that the Fourth Circuit has adopted the "strict liability" approach to inadvertent disclosures of attorney-client privileged information,[25] this court has observed that the issue of

---

[21] *Id.*

[22] *Id.* at 1356 (internal citations omitted).

[23] *Id.* at 1356; *citing In re Horowitz,* 482 F. 2d 72, 82 (2d Cir. 1973) (J. Friendly).

[24] *Id.* at 1357.

[25] Saltzburg et al, *supra,* §501.02[5][k][v] at 501-54.

inadvertent disclosure has not expressly been addressed by the Fourth Circuit.[26] The very uncertainty of the Fourth Circuit's position is grounds for proceeding cautiously, because if the *In re Grand Jury Proceedings* case does suggest that the court would take a strict liability approach, the waiver would be broad subject matter waiver, rather than waiver limited to the contents of the disclosed document. *In re Grand Jury Proceedings*, 727 F.2d at 1357. The Fourth Circuit's subsequent case, *Martin Marietta Corp. v. United States*, 856 F.2d 619 (4th Cir. 1988) is further grounds for caution with respect to the inadvertent waiver doctrine.[27]

In *Martin Marietta*, the Fourth Circuit again examined the attorney-client privilege and its waiver in the context of a criminal case. 856 F.2d 619 (4th Cir. 1988). The defendant in a mail fraud case sought to subpoena production from his employer certain documents that it had disclosed previously to the United States to settle criminal and administrative cases against it. *Id*. at 620. The employer resisted the subpoena arguing that the information sought was

---

[26] *F.C. Cycles Int'l Inc.*, 184 F.R.D. at 76 ("The defendant asserts that the United States Court of Appeals for the Fourth Circuit has adopted the middle-ground approach [to inadvertent waiver of attorney-client privileged material]. The Court has not expressly addressed this issue.").

[27] It should be noted that Fed. R. Evid. 501 provides that "in civil actions and proceedings, with respect to an element of a claim or defense as to which State law supplies the rule of decision, the privilege of a witness, person, government, State or political subdivision thereof shall be determined in accordance with State law." Thus, for diversity cases in this district in which Maryland law governs, state privilege law, not federal, governs. Maryland has adopted the "balancing approach" to inadvertent waiver of the attorney-client privilege. *Elkton Care Center Assocs. Ltd. P'Ship v. Quality Care Mgmt*., 145 Md. App. 532 (Md. Ct. Spec. App. 2002). *See also F.H. Chase, Inc. v. Clark/Gilford*, 341 F. Supp. 2d 562, 562 (D. Md. 2004) (applying the balancing test of *Elkton Care Center* in diversity contract case in federal court). Counsel must be cautious to make sure which standard governs in their cases, and in cases asserting both federal and state claims, both federal and state privilege standards could be applicable, which could result in the paradoxical situation in which a producing party's conduct could constitute waiver of the attorney-client privilege for the federal claims, but not for the state claims.

protected by the attorney-client privilege and work product doctrine. *Id*. The defendant responded that the prior disclosure waived the privilege and protection. *Id*. The Fourth Circuit examined whether the employer's prior production impliedly waived the privilege and protection. *Id*. at 621-23. It stated, relevantly:

> Implied waiver nullifies a privilege when disclosure of a privileged communication has vitiated confidentiality. Unlike express waiver which allocates control of the privilege between parties to the communication, implied waiver allocates control of the privilege between the judicial system and the party holding the privilege . . . . Martin Marietta argues for application of a limited implied waiver as to both privileges. Most courts continue to state the rule of implied waiver in absolute form – any disclosure of a confidential communication outside a privileged relationship will waive the privilege as to all information related to the same subject matter. That is commonly referred to as subject matter waiver as opposed to limited waiver for which Martin Marietta argues. However, competing policy concerns, such as facilitating the settlement of litigation, permitting full cooperation among joint defendants, expediting discovery and encouraging voluntary disclosure to regulatory agencies have led courts to carve out exceptions to the purportedly absolute rule of waiver . . . . The Fourth Circuit has previously rejected the limited waiver concept as to the attorney-client privilege and as to non-opinion work-product. We have embraced the limited waiver concept as to opinion work-product.

Id. at 623.

The lessons taught by the *In re Grand Jury Proceedings* and *Martin Marietta* cases are sobering to those with cases pending in the Fourth Circuit when considering the procedures suggested by the proposed changes to the rules of civil procedure to deal with the burdens and expense of privilege review related to discovery of voluminous electronically stored information. Both these cases were decided more than fifteen years ago, long before the problems associated with computer generated and stored information were on anyone's radar scope. Although both were decided in the context of grand jury investigations in criminal cases, neither confined its ruling to application of the privilege in that context, but, rather, spoke broadly in terms that

would apply equally to civil cases. Further, they clearly express a very strict interpretation of the attorney-client privilege, and an unambiguous willingness narrowly to confine it to its essential function - - preserving communications intended to be kept confidential. Finally, both cases take an unforgiving view of the results of its waiver - - subject matter waiver.

This case thus highlights an unavoidable clash of important policies. On the one hand is the substantive law narrowly confining the attorney-client privilege to its essential purpose, with subject-matter waiver as the price for unprotected disclosure. On the other is the distinct trend towards limiting the nature and amount of discovery to the needs of the particular case, given the issues in the case, the importance of the facts sought to be discovered, and the resources of the parties, such as embodied in Fed. R. Civ. P. 26(b)(2), and the proposed changes to the rules of civil procedure relating to discovery of electronically stored information. In attempting to resolve this clash, it is important to have a clear appreciation of what is at stake. This requires an awareness of the enormous costs that would accompany a requirement that in all civil cases the production of electronically stored information could not be accomplished until after a comprehensive privilege review and particularized assertion of privilege and work product claims.

The commentary to the proposed changes to Rules 16 and 26, quoted above, speak of the costs associated with discovery of electronically stored information in general, and privilege review prior to production specifically: “The volume of the information and the forms in which it is stored make privilege determinations more difficult and privilege review correspondingly

more expensive and time-consuming, yet less likely to detect all privileged information."[28] One does not have to look very hard to find specific cases that provide a factual basis for this concern. In *Rowe Entm't, Inc. v. The William Morris Agency, Inc.*, 205 F.R.D. 421 (S.D.N.Y. 2002) the court was faced with motions by defendants that sought to be protected from the burden and expense of producing e-mail that had been requested by the plaintiffs during discovery in a civil case. One defendant supported its motion with an estimate from a computer consultant that it would cost $395,944 to select, catalogue, restore, and process a limited sampling of the e-mails sought, and $9,750,000 to do the same for all e-mail requested. *Rowe Entm't*, 205 F.R.D. at 425. Another defendant produced cost estimates ranging from $43,110 to $84,060 to produce requested e-mail, with an estimated cost of $247,000 to review the e-mail for privilege and work-product prior to production. *Id*. A third estimated that it would take more than two years to retrieve and catalogue the e-mails requested by the plaintiff at a cost of $395,000, with an additional cost of $120,000 to conduct privilege review – which would take a full-time employee two years to complete. *Id*. at 426. In another case, *Zubulake v. UBS Warburg LLC*, 216 F.R.D. 280, 283 (S.D.N.Y. 2003) the defendant submitted cost estimates in support of its request to shift the production costs to the plaintiff of $165,954.67 to search for and restore responsive electronic information, with an additional estimated expense of $107,694.72 for attorney and paralegal review costs.

Those who bear the administrative and financial costs of responding to voluminous discovery requests for electronically stored information are mindful of the potential burden and

---

[28] Report of the Judicial Conference on Rules of Practice and Procedure to the Chief Justice of the United States, *supra*, at 27, n. 3.

expense. A publication of the Association for Information Systems (AIS) has observed:

> Broadly defined, e-evidence is electronically-stored information on any type of computer device that can be used as evidence in a legal action. Since e-mail can provide especially devastating evidence, the use of e-evidence is increasing. In a survey of 1,100 U.S. Companies conducted by the American Management Association and the ePolicy Institute, 14% of respondents said they were ordered by a court or regulator to produce employee e-mail in 2002, which was up from 9% in 2001.[29]

The same study estimates that "discovery of e-mail occurs in nearly 100% of federal civil . . . cases and major employment disputes,"[30] with the following impact on the responding party:

> Responding to a discovery request for a corporation's internal e-mail may seem simple and straightforward to the courts or lawyers. However, a company served with a request to produce e-mail messages faces time consuming and expensive processes. The cost and complexity depends on the volume of e-records, how they are organized, and their accessibility. The cost of responding to a discovery request can be in the millions of dollars if several years' worth of archived e-mail and files must be located, restored, sorted through and cleansed to remove non-relevant confidential material . . . . Those costs are often in the millions of dollars.[31]

Importantly, the foregoing costs must be borne before the lawyers begin the job of privilege review. With regard to the process of assembling electronic information responsive to discovery requests, an entire industry of consultants has developed to provide services to litigants.[32] Some consultants are nothing short of giddy in their projections of the expected fees to be earned from

---

[29] Linda Volonino, *Electronic Evidence and Computer Forensics*, 12 Communications of the Association for Information Systems 27, October 2003, at 7, available at http://cais.isworld.org/articles/12-27/article.pdf.

[30] *Id*. at 11.

[31] *Id*. at 14.

[32] "A cottage industry of companies assisting with the production and retrieval of electronic data and litigation has recently arisen." T. Delaney, *E-Mail Discovery: The Duties, Danger and Expense*, 46 Fed. Lawyer 42, 44 (Jan. 1999).

these services. For example, the reports of a survey conducted by a "digital discovery" consultant of users of consulting services led it to conclude "[b]ased on our research, we estimate that 2004 domestic commercial electronic discovery revenues were in the range of $832 million – a 94 percent increase from 2003."[33] Projections for the next three years were equally attention grabbing: 2005: $1.282 billion; 2006: $1.923 billion; and 2007: $2.865 billion.[34] It also is instructive to look back to see how quickly these costs have grown in such a short time. Estimated total revenues earned by consulting companies providing services to litigants regarding discovery of electronic information was:

1999: $40 million
2000: $70 million
2001: $150 million
2002: $270 million
2003: $430 million[35]

Despite the uncertainty regarding which approach to inadvertent disclosure of attorney-client privileged material would be adopted by the Fourth Circuit, there is a viable method of dealing with the practical challenges to privilege review of electronically stored information without running an unacceptable risk of subject-matter waiver. It lies with the courts issuing scheduling orders under Fed. R. Civ. P. 16, protective orders under Fed. R. Civ. P. 26(c), or discovery management orders under Fed. R. Civ. P. 26(b)(2) that incorporate procedures under

---

[33] Socha-Gelbmann 2005 Electronic Discovery Survey Results, http://www.sochaconsulting.com/2005surveyresults.htm.

[34] *Id.*

[35] Socha-Gelbmann 2004 Electronic Discovery Survey Results, http://www.sochaconsulting.com/Publications/DDEE%2005.03.pdf; Socha-Gelbmann 2004 Electronic Discovery Survey Results, http://www.sochaconsulting.com/Publications/LawTechnologyNews%20Article%208.04.pdf.

which electronic records will be produced without waiving privilege or work product that the courts have determined to be reasonable given the nature of the case, and that have been agreed to by the parties. This practice, already commonly followed in cases where discovery of electronic records is anticipated, is specifically encouraged by the proposed rule changes to the discovery rules now under review by the Supreme Court.[36] As will be seen, it is essential to the success of this approach in avoiding waiver that the production of inadvertently produced privileged electronic data must be at the compulsion of the court, rather than solely by the voluntary act of the producing party, and that the procedures agreed to by the parties and ordered by the court demonstrate that reasonable measures were taken to protect against waiver of privilege and work product protection. To appreciate how the process must work, one must understand Fed. R. Evid. 501, and the doctrine of compelled disclosure encompassed by Proposed, but not enacted, Rule of Evidence 512.

Fed. R. Evid. 501 states:

> Except as otherwise required by the Constitution of the United States or provided by Act of Congress or in rules prescribed by the Supreme Court pursuant to statutory authority, the privilege of a witness, person, government, State, or political subdivision thereof shall be governed by the principles of the common law as they may be interpreted by the courts of the United States *in the light of reason and experience*. However, in civil actions and proceedings, with respect to an element of a claim or defense as to which State law supplies the rule of decision, the privilege of a witness, person, government, State, or political subdivision thereof shall be determined in accordance with State law. (Emphasis added).

Therefore, it "authorizes federal courts to define new privileges by interpreting 'common law principles . . . in the light of reason and experience.'" *Jaffee v. Redmond,* 518 U.S. 1, 8 (1996).

---

[36] *Supra* n.3 and n.4.

And, because "'the common law is not immutable, but flexible, and by its own principles adapts itself to varying conditions,'" *Id.* (internal citations omitted), Rule 501 "did not freeze the law governing the privileges of witnesses in federal trials at a particular point in our history, but rather directed federal courts to 'continue the evolutionary development of testimonial privileges.'" *Id.* at 9.

Notably, when Congress elected to adopt the "general mandates" of Rule 501, it rejected a series of specific privilege rules that had been "formulated by the Judicial Conference Advisory Committee on the Rules of Evidence and approved by the Judicial Conference of the United States and by [the Supreme] Court." *Id*. at n.7. Many learned commentators have observed that, because the proposed evidence rules, often referred to as "standards," were approved by the Judicial Conference and the Supreme Court, they evidence the common law of privilege and therefore may be applied under Rule 501 if reason and experience make such application appropriate. *See* 3 Jack B. Weinstein & Margaret A. Berger, *Weinstein's Federal Evidence*, §512.02 (Joseph M. McLaughlin ed., Matthew Bender 2d ed. 1997 ("Supreme Court Standards are not part of the Federal Rules of Evidence. The Supreme Court originally proposed the Standards as Rules, but Congress struck them before enacting the other proposed rules into law. However, Supreme Court Standard 512 retains considerable utility as a guide to the federal common law referred to in Rule 501."); Graham, Handbook of Federal Evidence §501.1 (5th ed. 2001) ("While the nine rules recognizing specific privileges as drafted by the Advisory Committee and prescribed by the Supreme Court do not have the force of law, they do provide standards reflective of the 'reason and experience' mentioned in Rule 501. These nine specific provisions relating to privilege, . . . , are consistent and co-extensive with privileges recognized

by the federal common law. The remaining proposed rules, now Standards, deal with procedural aspects governing all privileges, no matter their source of origin . . . . Standard 512 provides an exception for disclosure where compelled or made without opportunity to claim."); Saltzburg, et al., Federal Rules of Evidence Manual § 501.02[3] ("While common-law development is now mandated, the question remains whether the Federal Courts in developing the law of privileges should consider the proposed-but-rejected privileges as either persuasive or controlling. Most Courts have held that the recommendations of the Advisory Committee and the Supreme Court are a useful guide, though not controlling in determining the existence and scope of a federal privilege.").

As noted in the above cited authorities, one of the proposed rules, Standard 512, is especially relevant to this case. It states: "[e]vidence of a statement or other disclosure of privileged matter is not admissible against the holder of the privilege if the disclosure was (a) compelled erroneously or (b) made without opportunity to claim the privilege." Proposed Rule 512, 56 F.R.D. at 259. The commentary to proposed Rule 512 recognized that it cannot undo the damage that inadvertent disclosure of privileged information causes, but it can contain it. "Confidentiality, once destroyed, is not susceptible of restoration, yet some measures of repair may be accomplished by preventing uses of the evidence against the holder of the privilege. The remedy of exclusion is therefore made available when the earlier disclosure was compelled erroneously or without opportunity to claim the privilege." *Id*.

Federal courts also have referenced Proposed Rule 512 in contexts that are relevant to this case, to hold that a party that is compelled to produce privileged material, or erroneously produces it, does not waive the privilege. In *Transamerica Computer Co. v. IBM*, 573 F.2d 646

(9th Cir. 1978), the Ninth Circuit held that IBM had not waived its privilege claims to records that erroneously had been produced in prior litigation involving different parties, because the production was in response to an accelerated discovery schedule that the trial court had imposed, and the disclosures had been unintentional. Notably, the court observed that in the earlier litigation, IBM had produced 17 million pages of documents during a court ordered production schedule that had "dramatically accelerated the document inspection program." *Transamerica*, 573 F.2d at 648. The court noted that during this demanding production schedule, IBM had undertaken "herculean" efforts to review documents for privilege." *Id.* at 648-49. Therefore, it had not been guilty of any want of diligence. Of greater importance, however, was the fact that the trial judge had ruled that "the inadvertent production of allegedly privileged material by either party would not constitute a waiver of that party's right to claim the attorney-client privilege, provided only that the party disclaiming waiver had continued to employ procedures reasonably designed to screen out privileged material." *Id.* at 649-50.

In concluding that IBM had not waived its privilege claims by producing the documents in the earlier litigation, and therefore could not be compelled by *Transamerica* in the subsequent litigation to produce it, the Ninth Circuit declined to view the issue solely as one of inadvertent disclosure, but rather focused on the importance of the court's compulsion of the production of the documents under conditions that unavoidably resulted in disclosure of some privileged material. The court observed:

> We do not decide, however, whether this sort of 'inadvertent' disclosure constitutes a waiver of the attorney-client privilege, for we believe that this case is properly decided upon the basis of a legal principle upon which the parties are in complete accord. Specifically, IBM asserts, and [Transamerica] concedes, that a party does not waive the attorney-client privilege for documents that he is *compelled* to produce.

Id. at 650-51. In reaching its decision, the Ninth Circuit relied on proposed Rule 512: "Proposed Rule 512 is perhaps even more on point. This proposed rule would have prohibited the use of any privileged matter if its disclosure had been 'compelled erroneously' or had been 'made without opportunity to claim the privilege.' It is our belief that under the specific circumstances of the accelerated discovery proceedings in the CDC litigation, IBM's inadvertent production there of some privileged documents does not constitute a waiver of the privilege protecting the production of those documents, for that production was 'made without (adequate) opportunity to claim the privilege.'" *Id.* at 651.

Also central to the court's ruling was its recognition that the production of some privileged material by IBM had occurred as a result of the trial court's discovery order:

> As the judicial officer directly in charge of supervising the discovery proceedings in that litigation . . . [the trial judge] was in an ideal position to determine whether the timetable he himself had imposed was so stringent that, as a practical matter, it effectively denied IBM the opportunity to claim the attorney-client privilege for documents it was producing for inspection by CDC. TCC acknowledges that waiver cannot be directly compelled, and . . . [the judge's] rulings recognize and we so hold, that neither can it be indirectly compelled.

Id. at 652.

Finally, the court noted that the trial judge had further issued a ruling "explicitly protecting and preserving all claims of privilege, provided only that the parties wishing to preserve privilege had engaged in suitable screening techniques." *Id.*

Subsequent courts have applied the ruling of *Transamerica* or independently referred to Proposed Rule 512 in instances where a party had been compelled to produce privileged material erroneously, or without adequate opportunity to review it for privilege. *Sangre de Cristo*

Community Mental Health Serv., Inc. v. United States, 723 F.2d 1461, 1466 (10th Cir. 1983) ("production of privileged documents by an attorney under court order does not necessarily constitute a waiver of the privilege," *citing* Proposed Rule 512, "[a]lthough Congress did not enact rule 512, it still has utility as a standard of law on the privileges that should be applied in federal courts." (internal citations omitted)); *Georgetown Manor, Inc. v. Ethan Allen Inc*., 753 F. Supp. 936, 938, n.4 (S.D. Florida, 1991) (*citing Transamerica*); and *Little v. Brown & Williamson Tobacco Corp*., Nos. 2:98-1879-23 and 2:98-3235-23, 1999 WL 33591437, at * 3 (D.S.C. Oct. 25, 1999) (noting that Proposed Rule 512 may have utility in determining federal common law of privilege); *Amway Corp. v. Proctor & Gamble Co.*, No. 1:98-CV-726, 2001 WL 1818698, at *2 (W.D. Mich April 13, 2001) (noting court decisions holding that privilege is not lost if disclosure was compelled erroneously or if holder did not have opportunity to assert privilege, citing treatises, case law)[37]; .

The *Transamerica* case and those that have followed it would allow parties that have entered into an agreement to preserve privilege claims with respect to production of electronically stored information to avoid subsequent claims by third parties that the production waived the privilege, provided: (a) the party claiming the privilege took reasonable steps given the volume of electronically stored data to be reviewed, the time permitted in the scheduling order to do so, and the resources of the producing party; (b) the producing party took reasonable steps to assert promptly the privilege once it learned that some privileged information

[37] No decision from the Fourth Circuit has been found discussing whether Proposed Rule 512 constitutes the "common law" of privilege under Rule 501. However, in *Farnsworth Cannon v. Grimes*, 635 F.2d 268, 270-71, n.8 (4th Cir. 1980), the Fourth Circuit did recognize that proposed privilege rule 509(e) (state secrets privilege) was part of the common law of privilege despite the fact that it had not been adopted.

inadvertently had been disclosed, despite the exercise of reasonable measures to screen for privilege and, importantly; (c) the production had been compelled by court order that was issued after the court's independent evaluation of the scope of electronic discovery permitted, the reasonableness of the procedures the producing party took to screen out privileged material or assert post-production claims upon discovery of inadvertent production of privileged information, and the amount of time that the court allowed the producing party to spend on the production. Thus, the *Transamerica* case provides a method to meet the goals of the proposed changes to the Federal Rules of Civil Procedure regarding preservation of privilege claims during production of electronically stored material within the context of existing substantive privilege law, which the proposed rule changes cannot trump.

And, even the D.C. Circuit, one of the staunchest adherents to the "strict accountability" approach to waiver of privileged material, has recognized in an analogous context that production of privileged information under circumstances where the party asserting the privilege is unable effectively to prevent the disclosures or to assert the privilege, does not result in waiver.

In *Securities and Exchange Commission v. Lavin*, 111 F.3d 921 (D.C. Cir. 1997), the D.C. Circuit examined whether the production of tapes of communications between a security trader and his wife, assertedly protected by the marital communications privilege, by the husband's employer that had retained copies of the tapes, waived the privilege. Importantly, the court recognized that the issue involved more than the concept of inadvertent production of privileged material by the holder of the privilege or its attorney. Rather, the court observed:

> the question of the Lavins' alleged waiver arises in an unusual context, different from that of any of the cases on which the district court and the parties rely. The

> Lavins assert the privilege with regard to communications, the physical manifestations of which belong to a third party, Mr. Lavin's employer. Consequently, the cases cited that discuss implied waiver when the holder of the privilege or his attorney is in possession of the materials at issue and fails to take adequate precautions to maintain their confidentiality, i.e. negligent or inadvertent disclosures, offer limited guidance on whether disclosure by third parties over whom the holder of the privilege has virtually no control . . . may nonetheless be held to constitute waiver. *In cases of involuntary disclosures, at least one court has held that waiver occurs only when the holder has failed to take reasonable steps to reclaim the protected material.*

Lavin, 111 F.3d at 929-30 (emphasis added). The D.C. Circuit adopted the following language from a Ninth Circuit opinion, *United States v. de la Jara*, 973 F.2d 746 (9th Cir. 1992):

> [W]hen the disclosure of privileged material is involuntary, we will find the privilege preserved if the privilege holder has made efforts 'reasonably designed' to protect and preserve the privilege. Conversely, we will deem the privilege to be waived if the privilege holder fails to pursue all reasonable means of preserving the confidentiality of the privileged matter.

Lavin, 111 F.3d at 930, *citing de la Jara*, 973 F.2d at 749. The *Lavin* court further explained its ruling in language that is equally instructive to this case:

> In our view the Ninth Circuit's standard with regard to involuntary disclosures strikes the proper balance between the conflicting policies of facilitating truth-seeking by construing privileges strictly and, at the same time, fairly and adequately 'protecting the privacy of marriage and encouraging open and frank communications . . . . *In light of the modern regulatory age and technological advances, moreover, such an approach is necessary precisely because the ability to protect against all disclosures is becoming increasingly elusive . . . Unless communications remain privileged as long as the holder has acted reasonably in attempting to protect them, involuntary disclosures by third parties may render illusory the privilege's guarantee of privacy.*

Lavin, 111 F.3d at 930 (emphasis added) (internal citations omitted).

This observation from one of the strongest proponents of the strict accountability doctrine of privilege waiver is significant. There is little conceptual difference between the nonconsensual disclosure of privileged material by a third party over whom the privilege holder

has no control, and involuntary production by a party ordered to produce voluminous materials by court order that requires disclosure within a time frame that, despite reasonable screening, prevents unrestricted opportunity to review for privilege. In either instance, provided the holder of the privilege has taken all reasonable measures under the circumstances to prevent disclosure, but was prevented from doing so by matters beyond his control, a finding of waiver would be unfair and improper. Further, the D.C. Circuit recognized what is painfully apparent in a world where almost all writings are generated and stored electronically, and far more widely disseminated than in the days of "paper documents" – technological advances have made it increasingly difficult to protect against all involuntary disclosures. If, indeed, the common law of privilege is not frozen in antiquity, but rather is flexible and adaptable to changing circumstances,[38] then it must be elastic enough to permit reasonable measures to facilitate production of voluminous electronically stored information during discovery without imposing on the parties unreasonable burdens on their human and fiscal resources. The unavoidable truth is that it is no longer remarkable that electronic document discovery may encompass hundreds of thousands, if not millions, of electronic records that are potentially discoverable under Rule 26(b)(1). In this environment, to insist in every case upon "old world" record-by-record pre-production privilege review, on pain of subject matter waiver, would impose upon parties costs of production that bear no proportionality to what is at stake in the litigation, and mark a dramatic retreat from the commendable efforts since the adoption of Rule 26(b)(2) to tailor the methods and costs of discovery to fit the case at hand. And, of equal importance, a failure to adapt to current "real world" discovery realities will unacceptably lengthen pretrial discovery,

[38] *Jaffe*, 518 U.S. at 8.

because courts cannot insist upon such painstaking and costly review unless they are willing to allow enough time to do so reasonably. It is unlikely that courts are going to embrace the notion of years-long timetables to allow parties to assemble and review voluminous electronic information prior to production during discovery.

The foregoing discussion of Rule 501, Proposed Rule 512, and the *Transamerica* and *Lavin* cases teach valuable lessons to apply to the challenges presented in this, and most cases, regarding the discovery of electronically stored information. First, to the extent that parties already are negotiating "non-waiver" electronic records production agreements, a practice encouraged by the proposed changes to Rule 16(f), they would be unwise to assume that such agreements will excuse them from undertaking any pre-production privilege review, or doing less of a pre-production review than is reasonable under the circumstances. In circuits that have adopted the "strict waiver" approach to inadvertent production, such an agreement would be fatal. And, even in those jurisdictions that have adopted the more lenient "balancing test," the producing party still must show that reasonable measures were taken to screen for privileged information.[39] The better approach is to assume that complete pre-production privilege review is

[39] A casual reading of the proposed changes to Rules 16 and 26 and their accompanying commentary, without evaluation of the governing substantive law of privilege waiver, could lead counsel to conclude that the proposed rules permit them to, with a wink and a nod, forego reasonable pre-production review altogether, or to do only a cursory screening. This would be a mistake. Reviewing appellate courts are unlikely to accept the doctrine of compelled disclosure under Proposed Rule 512 if it is offered to justify transparently inadequate pre- and post-production privilege review and assertion. If the producing party had adequate opportunity to do full pre-production review, or greater privilege review than was done, but, through sloppiness or want of diligence failed to do so, the reviewing court is unlikely to find present the level of compulsion necessary to immunize the production from waiving privilege. Similarly, absent any clear signal from the appellate courts that they should do otherwise, district courts called upon to "bless" the production procedures agreed upon by counsel with a court order should independently satisfy themselves that full privilege review reasonably cannot be accomplished

required, unless it can be demonstrated with particularity that it would be unduly burdensome or expensive to do so.

The cost-benefit balancing factors listed in Rule 26(b)(2) provide useful analytical tools to enable a producing party to marshal the specific facts that would justify less than full pre-production privilege review. The amount of discovery of electronically stored information that should be permitted in a particular case will be a function of the issues in the litigation, the resources of the parties, whether the discovery sought is available from alternative sources that are less burdensome, and the importance of the evidence sought to be discovered by the requesting party to its ability to prove its claims. As this court noted in *Thompson v. HUD*, 219 F.R.D. 93 (D. Md. 2003), courts have nearly limitless ability under Rule 26(b)(2) to fashion reasonable limits to potentially burdensome discovery requests, but the parties must get beyond the posturing that all too often takes place and provide the court with particularized information and reasonable suggestions how to do so.

In this case the BCPD did file an affidavit intended to particularize the unreasonable burden that would result from producing all of the records sought by the Plaintiffs in their Rule 34 requests. However, it was less complete than it should have been. It did identify the limited number of information technology personnel available to conduct the search for electronic records, and the competing demands on their services within the police department, but it failed to estimate the number of hours that would be required for them to conduct the requested review,

---

within the amount of time court allowing for the production. The court also should satisfy itself that the procedures agreed upon by counsel regarding privilege production are in fact reasonable and that more could not be accomplished within the production period given the scope of electronic records production permitted by the court.

or to sufficiently demonstrate how this would impact adversely the fiscal and operational capabilities of the police department. A party that seeks an order from the court that will allow it to lessen the burden of responding to allegedly burdensome electronic records discovery bears the burden of particularly demonstrating that burden and of providing suggested alternatives that reasonably accommodate the requesting party's legitimate discovery needs.

Second, as this case graphically demonstrates, it is no longer acceptable for the parties to defer good faith discussion of how to approach discovery of electronic records until they have complied with the briefing schedule in Local Rule 104.8. Rather, as the proposed changes to Rule 16(f) make clear, counsel have a duty to take the initiative in meeting and conferring to plan for appropriate discovery of electronically stored information at the commencement of any case in which electronic records will be sought. In the absence of any guidance in the court's scheduling order, or in the local rules of court, the parties are not without resources that will assist them in determining what to discuss at their meeting. Indeed, the newly revised Civil Discovery Standards for the American Bar Association Section on Litigation[40] contain detailed information about the issues that the parties should discus in their effort to agree upon an electronic records discovery plan. At a minimum, they should discuss: the type of information technology systems in use and the persons most knowledgeable in their operation; preservation of electronically stored information that may be relevant to the litigation; the scope of the electronic records sought (i.e. e-mail, voice mail, archived data, back-up or disaster recovery data, laptops, personal computers, PDA's, deleted data) the format in which production will occur (will records be produced in "native" or searchable format, or image only; is metadata

[40] *American Bar Association Civil Discovery Standards* 29, amend. August 2004.

sought); whether the requesting party seeks to conduct any testing or sampling of the producing party's IT system; the burdens and expenses that the producing party will face based on the Rule 26(b)(2) factors, and how they may be reduced (i.e. limiting the time period for which discovery is sought, limiting the amount of hours the producing party must spend searching, compiling and reviewing electronic records, using sampling to search, rather than searching all records, shifting to the producing party some of the production costs); the amount of pre-production privilege review that is reasonable for the producing party to undertake, and measures to preserve post-production assertion of privilege within a reasonable time; and any protective orders or confidentiality orders that should be in place regarding who may have access to information that is produced.

It cannot be emphasized enough that the goal of the meeting to discuss discovery is to reach an agreement that then can be proposed to the court. The days when the requesting party can expect to "get it all" and the producing party to produce whatever they feel like producing are long gone. In many cases, such as employment discrimination cases or civil rights cases, electronic discovery is not played on a level field. The plaintiff typically has relatively few electronically stored records, while the defendant often has an immense volume of it. In such cases, it is incumbent upon the plaintiff to have reasonable expectations as to what should be produced by the defendant.

In this case, the Plaintiffs filed voluminous and detailed Rule 33 and 34 discovery requests that clearly identified their interest in discovering electronically stored information. The Defendants' immediate response should have been to invite the Plaintiffs to meet to discuss a reasonable discovery plan. Instead, objections first were raised, many of them boilerplate and

conclusory, in the Defendants' answers to the discovery requests. The Plaintiffs responded with multiple written communications outlining their objections to the Defendants responses. When impasse was not overcome, the Plaintiffs followed the procedures in Local Rule 104.8 and prepared and served a motion to compel. Only when that motion was fully briefed was it filed with the court. An expedited hearing was held, but even so, months had passed from the commencement of discovery while the dispute festered. Such delay is no longer acceptable, and it is the duty of the parties to initiate the negotiation process if the court has not ordered it. As I ordered during the hearing, the meeting that should have occurred months ago will be held within 30 days. A follow-up hearing with the court will be scheduled at which time a reasonable electronic discovery plan will be ordered.

One of the issues the parties were ordered to discuss was the nature of privilege review the Defendant would undertake, both pre- and post-production. The Defendants were advised that they bore the burden of demonstrating with particularity the need for less than full pre-production privilege review, as well as of proposing reasonable alternatives. I advised the parties that at the follow-up hearings, I would issue an order that compelled production of electronic records within a specific time that is reasonable. I also stated that I would independently determine, using the Rule 26(b)(2) factors, the amount of electronic discovery that would be permitted; whether less than full privilege review was reasonable given the extent of electronic discovery allowed and the time to do so and, if full privilege review was not feasible, whether the procedures agreed to by counsel are reasonable. If so, I will issue an order approving them that includes language that compliance with the approved procedures will not result in the waiver of any privilege or work product claim for any inadvertently produced

privileged material. As I stated during the hearing, the issuance of such an order is essential to protecting against subject matter waiver of attorney-client privileged or work product protected information. In this regard I am persuaded that the holding in the *Transamerica* case is correct, and that Proposed Rule 512 is part of the common law of privilege that may be recognized by this court under Rule 501, because both reason and experience militate in favor of its application under the facts of this case. If I eventually am proved wrong, then the Defendants still will be able to argue that their production of privileged information was under the erroneous belief that this order immunized them from waiver, as Proposed Rule 512 speaks both to production compelled without adequate opportunity to raise privilege claims, as well as erroneous production of privileged information.[41]

It is so ordered.

_____ _____/s/_____
Date Paul W. Grimm
United State Magistrate Judge

[41] 24 Charles Alan Wright & Kenneth W. Graham, *Federal Rules of Evidence*, Ch. 6 § 5507, 579 and 579 n. 122 (1986). Thus, even the treatise most openly critical of trial courts' approval of agreements between parties to produce discovery without full privilege review acknowledges that the producing party who was subject to such an order has a viable defense under the concept of "erroneous production" against a subsequent opposing party that claims that the privilege was waived.

AIN THE UNITED STATES DISTRICT COURT

DISTRICT OF UTAH, NORTHERN DIVISION

PHILLIP M. ADAMS & ASSOCIATES, L.L.C., a Utah Limited Liability Company, Plaintiff, vs. DELL, INC., FUJITSU LIMITED, FUJITSU COMPUTER SYSTEMS CORP., MPC COMPUTERS, LLC, SONY ELECTRONICS INC., WINBOND ELECTRONICS CORP., ASUSTEK COMPUTER, INC., ASUS COMPUTER INTERNATIONAL, QUANTA COMPUTER, INC, QUANTA COMPUTER USA, INC., QUANTA MANUFACTURING, INC., MICRO-STAR INTERNATIONAL CORPORATION, LTD., MSI COMPUTER CORPORATION, NATIONAL SEMICONDUCTOR CORPORATION, Defendants. And Related Third-Party Claims.	MEMORANDUM DECISION AND ORDER: • GRANTING IN PART [492] MOTION FOR TERMINATING SANCTIONS AGAINST ASUS BASED UPON ASUS' SPOLIATION OF EVIDENCE OF ITS PIRACY; • GRANTING IN PART [559] MOTION TO STRIKE; and • DENYING [604] MOTION TO STRIKE Case No. 1:05-CV-64 TS The Honorable Ted Stewart Magistrate Judge David Nuffer

Phillip M. Adams & Associates (Adams) moved for entry of judgment for liability against defendants ASUSTEK Computer, Inc. and ASUS Computer International (collectively ASUS) based upon ASUS' alleged spoliation of evidence.[1] ASUS has responded with two motions to strike evidence upon which Adams' motion relies for purposes of this motion.[2] This order grants the motion for sanctions in part; grants in part the motion to strike the Woon Report for purposes of this motion; and denies the motion to strike certain emails and the printout of program headers.

[1] Adams' Motion for Terminating Sanctions Against ASUS Based upon ASUS' Spoliation of Evidence of Its Piracy, docket no. 492, filed April 17, 2008.

[2] ASUSTeK's Motion to Strike Exhibit E to Plaintiff's Memorandum in Support of Its Motion for Terminating Sanctions, docket no. 559, filed June 30, 2008; ASUSTeK's Motion to Strike Exhibits A, B, C, D and I and Related (footnote continued)

Table of Contents

NATURE OF THE CASE 1

RELEVANT FACTS ON THIS MOTION 2

- Assertion of Infringement 3
  - Materials from Winbond 4
  - Materials from ASUS 6
  - Conclusions from the Evidence – and Adams' Arguments 7
- Assertion of Destruction of Evidence 9
  - ASUS' Data Resources 10

MOTIONS TO STRIKE 11

- Waiver of Motion to Strike Emails and Program Header Printouts 12
- Authentication 12
- Hearsay 15
  - Woon Report 15
  - Winbond Emails 17
  - Program Headers 18
- Confusion and Prejudice – Program Headers 19
- Summary of Remaining Evidence on this Motion 20

MOTION FOR SANCTIONS 22

- Unavailable Evidence 22
- Duty to Preserve 24
  - Adams' Notice to ASUS 24
  - Adams' Delay 25
  - When Did the Duty To Preserve Arise? 25
- Safe Harbor 27
- What Sanction is Appropriate? 29
  - Culpability 29
  - Prejudice 32

ORDER 33

Arguments in Plaintiff's Memoranda in Support of Its Motion for Terminating Sanctions Against ASUSTeK, docket no. 604, filed August 21, 2008.

Nature of the Case

In the late 1980s, Dr. Phillip Adams identified a defect in the NEC 765A floppy disk controller (FDC) which was a part of most personal computers.[3] Dr. Adams believed that the defect in the FDC could cause the random destruction or corruption of data without proper notification to the user that data had been destroyed, which potentially could lead to serious consequences.[4] After his discovery of the defect, Dr. Adams devoted substantial amounts of time and effort to developing various solutions to detect and resolve FDC defects.[5] Dr. Adams decided to patent the computer technology resulting from his development efforts, with the first patent application being filed in 1992.[6] To date, there have been at least five patents issued as the result of Dr. Adams' efforts.[7] Each of those patents has been purportedly assigned to Phillip M. Adams & Associates LLC, the Plaintiff in this case.[8]

The FDC-related defects have given rise to multiple lawsuits over the past several years, one of which culminated in October 1999 with a $2.1 billion class-action settlement by Toshiba.[9] In the aftermath of that class-action settlement, interest in Adams' technology allegedly increased resulting in licenses and infringement. Alleged misuse of Adams' technology has given rise to Adams' instant lawsuit. Adams previously filed a lawsuit against Gateway, Inc.

---

[3] Second Amended Complaint at 3, docket no. 222, filed January 4, 2007.

[4] *Id.*

[5] *Id.* at 2.

[6] U.S. Patent No. 5,379,414.

[7] Second Amended Complaint at 2.

[8] *Id.* at 3.

[9] Adams' Memorandum in Support of Its Motion for Terminating Sanctions Against ASUS Based upon ASUS' Spoliation of Evidence of Its Piracy (Memorandum in Support) at iv, docket no 493, filed April 17, 2008.

(Gateway) in this court[10] on similar grounds. That case (Gateway Case) was litigated long and hard but settled at trial.[11]

In this case, Adams alleges that ASUS, among other defendants, has infringed on his patents. Adams claims that ASUS obtained Adams' programs in early 2000; illegally used them to test ASUS motherboards; and reverse-engineered new software which it tried to patent.[12] Adams claims that ASUS required Winbond, a chip manufacturer, to modify the chips Winbond sold to ASUS, again using Adams' technology.[13] ASUS and Winbond are upstream suppliers to computer manufacturers.[14]

Relevant Facts on this Motion

Adams alleges that "ASUS has destroyed the source code and documents relating to [two] test programs" created with "Adams' patented and proprietary technology . . . ."[15] Adams also claims ASUS destroyed "documents that would have conclusively demonstrated ASUS' piracy."[16]

Adams' stated factual basis for this motion is twofold: first, that ASUS has illegally used Adams' patented software; and second, that ASUS has destroyed evidence of that use. The first assertion is identical to the liability issue in this case. The second assertion is premised on the first: Assuming ASUS *used* Adams' software, ASUS' *failure to produce evidence* of that use is

---

[10] *Adams v. Gateway*, Case No. 2:02-CV-106 TS, District of Utah.

[11] Minute Entries, docket nos. 563 and 564, filed April 4, 2006, *Adams v. Gateway*, Case No. 2:02-CV-106 TS, District of Utah.

[12] Memorandum in Support at iv-v.

[13] *Id.* at v.

[14] *Id.* at vi-vii.

[15] *Id.* at 1.

[16] *Id.*

sanctionable spoliation. Adams has no direct proof of destruction of evidence but is inferring destruction or withholding of evidence. Since Adams is convinced that ASUS infringed, Adams is also convinced that failure to produce evidence of infringement is sanctionable.

In discovery and ensuing correspondence to resolve discovery disputes, Adams requested that ASUS produce:

- Adams' detector programs;
- ASUS' detector programs that are based on Adams' detector;
- Correspondence with ASUS' suppliers and customers; and
- Documents relating to testing and modifications.[17]

In a protective order that limited some of Adams' discovery requests sent to ASUS, the court effectively approved Adams' requests that the foregoing materials be produced.[18] When ASUS' production of items in the foregoing categories was meager, Adams filed this motion.

Assertion of Infringement

Adams' first assertion is that ASUS "obtained Adams proprietary test programs . . . and then illegally used, dissected, reproduced and promulgated those programs and their derivatives . . . ."[19]

> ASUS' engineer, Sam Yang, reverse–engineered the Adams test program . . . and subsequently wrote his own testing programs that ASUS named "ifdc.exe" and "w2sec.exe." ASUS then required Winbond to modify its chips and to replace the defective Rev. C chip with an infringing Rev. G chip on its motherboards. ASUS

[17] The various requests for production are summarized in Memorandum in Support at xiii. *See* ASUS' corresponding narrative in ASUS' Memorandum in Opposition to Adams' Motion for Terminating Sanctions Against ASUSTeK (Memorandum in Opposition) at xviii, docket no. 561 filed June 30, 2008.

[18] Memorandum Decision and Order Granting in Part ASUSTeK's Motion for a More Definite Statement and Motion for Protective Order . . . ., docket no. 431, filed January 22, 2008.

[19] Memorandum in Support at iv.

directed all this activity under the threat of taking its business away from Winbond.[20]

To support anassertion of infringement, and to lay the foundation for a claim of spoliation, Adams relied in the original briefing on materials obtained from Winbond in the Gateway litigation.[21] These are four emails; a test report; a program file; and headers from source code files. Adams also relied on an ASUS patent application. Later, Adams supplemented his briefing with two emails produced by ASUS.

Materials from Winbond

A listing of the emails and the language Adams cites to show that ASUS used a test program follows:

Exhibit	Cited Language
Email PM Chen to YC Lu and others, January 31, 2000 4:39 PM[22]	We have tested [Winbond chip] 787IF with Asus' special S/W and found it fail [sic] in even worse condition. This matter is "LIFE-OR-DEATH" to the I/O business. We can never overemphasize it....
Email from PM Chen to YC Lu and others, January 27, 2000 4:07 PM[23]	The solution should be in two ways – 1) HP Case – Solution to solve the FDC failure for those PC shipped to the market or help HP/Asus to win the suit. 2) I/O revision -- How to fix our bug? Asus people just called me and asked us to provide the schedule...

[20] Memorandum in Support at v (emphasis omitted and paragraphs collapsed).

[21] *Id.* at x.

[22] Exhibit A to Adam's Memorandum in Support, filed under seal in docket no 494, filed April 17, 2008. The document has Bates No. WINBO 00075.

[23] Exhibit B to Adam's Memorandum in Support, filed under seal in docket no 494, filed April 17, 2008. The document has Bates No. WINBO 00076.

Exhibit	Cited Language
Email from PM Chen to LH Chen and others, January 27, 2000 1:41 PM[24]	Some HP people are visiting Asus to identify the failure mode…HP, Asus, Winbond, we have to treat this quite carefully and with highest priority to solve this headache.
Email LH Hsu to YC Peng and others February 8, 2000 4:35 PM[25]	The U.S. 5379414 [Adams'] patent has claim [sic] this similar solution. I will discuss with AE00 to avoid infringement.

While some of the foregoing documents refer to ASUS, they are all "emails between Winbond employees."[26]

The fifth document relied on in Adams' original briefing (the Woon Report) is written by a Gateway engineer who is alleged to have "participated in testing" with ASUS.[27] The portion of the report cited by Adams is:

Test Report, YC Woon July 31, 2000[28]	Apparently the utility's algorithm originated from one of IBM's consulting firm.[sic] ASUS wrote software using the same algorithm and use it to test the boards in ASUS. As this is a propriety software, and also due to its patented algorithm, the software could not be released to be used outside of ASUS. Winbond apparently got hold of the software through ASUS as they bought the same Winbond chip from them.

The Woon Report refers to two programs which comprise a utility which the report states "ASUS wrote using the same algorithm" that "originated from one of IBM's consulting firm.

[24] Exhibit C to Adam's Memorandum in Support, filed under seal in docket no 494, filed April 17, 2008. The document has Bates No. WINBO 00077.

[25] Exhibit D to Adam's Memorandum in Support, filed under seal in docket no 494, filed April 17, 2008. The document has Bates No. WINBO 00079.

[26] Memorandum in Support at viii.

[27] Memorandum in Support at ix.

[sic]"[29] Dr. Phillip Adams was a former IBM employee and Adams claims that "Winbond typically referred to Dr. Adams as "IBM's consulting firm."[30] The two programs which the Woon Report says ASUS wrote are referenced in the report as "ifdc.exe" and "w2sec.exe."[31] All the foregoing documents are from the year 2000.

In the Gateway litigation in late 2005, Winbond identified "an error detection program from ASUS."[32] In 2008, after some dispute, Winbond produced two programs, "ifdc.exe" and "w4sec.exe"[33] that Winbond says came from ASUS. This was executable code; not source code. Adams also relies on printouts of the headers from the "ifdc.exe" and "w4sec.exe" programs. [34] "Both programs include the notation: 'Programming by Sam Yang@ASUS.'"[35]

Materials from ASUS

Adams also relies on a patent application by ASUS[36] in late 2001 showing that ASUS attempted to patent "[a] method for preventing data corruption in a Floppy Diskette Controller . . . ."[37] This document was produced by ASUS.[38] "This application identifies the inventor of its subject matter as Jin-Hsin Yang, also known as Sam Yang."[39]

---

[28] The Woon Report is Exhibit E to Adam's Memorandum in Support, filed under seal in docket no 494, filed April 17, 2008.

[29] Woon Report at 1

[30] Memorandum in Support at ix.

[31] Woon Report at 2.

[32] Letter from Alfredo A. Bismonte to John R. Posthumus and Greory Philipps [sic], November 4, 2005, attached as Exhibit H to Memorandum in Support.

[33] Memorandum in Support at xii.

[34] Adams attached the program header printouts as Exhibit I to Memorandum in Support.

[35] Memorandum in Support at xii.

[36] The patent application is attached as Exhibit G to Memorandum in Support.

[37] *Id.* at I.

[38] Memorandum in Support at xi.

[39] *Id.* at xi.

ASUS produced a software program "ifdc.exe"[40] but only in executable form.[41] No source code[42] was produced.

In later supplemental briefing, Adams has identified two emails produced by ASUS as providing further support for his position that ASUS used a detector. In the first, Sam Yang states "I have finished the programming. The two programs is [sic] used to verify the FDC."[43] The email attaches ifdc.exe and w4sec.exe and describes the technical detail of how these programs work. Another email from Yang to the same recipient sent later that same day states "The program is updated. We can see the FDC problem easily by the two programs."[44] This email attaches ifdc.exe and w2sec.exe.

Conclusions from the Evidence – and Adams' Arguments

Adams has produced evidence which shows that in late 2000 Sam Yang aka Jin-Hsin Yang, an ASUS employee, developed programs to test floppy disk controllers; that Winbond regarded ASUS' test software as "special" and thought there was some issue of infringement; and that a Gateway engineer believed that ASUS wrote the software based on an algorithm developed by an IBM consultant and that Winbond was using that software.

Adams' argument goes beyond this evidence, however. Adams alleges *infringement* is demonstrated by these materials.

---

[40] Memorandum in Oppostion at xx.

[41] Memorandum in Support at x.

[42] A computer program's source code is the collection of files needed to convert from human-readable form to some kind of computer-executable form. The source code may be converted into an executable file by a compiler, or executed on the fly from the human readable form with the aid of an interpreter.

"Source Code," Wikipedia (last visited January 2, 2009).

[43] Email January 27, 2000 9:18 am, Sam Yang to Max Lu, attached as Exhibit 1 to Adams' Supplementation Regarding (1) ASUS' Spoliated and Infringing Detector, and (2) YC Woon's Test Report (Adams' Supplementation), docket no. 675, filed under seal December 29, 2008.

[44] Email January 27, 2000 1:26 pm, Sam Yang to Max Lu, attached as Exhibit 2 to Adams' Supplementation.

> Sometime in early 2000, ASUS *obtained* Adams proprietary test programs . . . and then *illegally used, dissected, reproduced and promulgated those programs* and their derivatives.[45]
>
> ASUS' engineer, Sam Yang, *reverse–engineered* the Adams test program that Adams had licensed to HP, and subsequently wrote his own testing programs that ASUS named "ifdc.exe" and "w2sec.exe."[46]
>
> This [patent] application shows beyond dispute that *ASUS had a copy of Dr. Adams' proprietary test programs, closely examined and reverse engineered those test programs, misappropriated the trade secrets* in them to create its own test programs, and then raced to the United States Patent Office to try to patent them.[47]

Adams does not support these infringement allegations with evidence. There is no direct evidence that ASUS possessed or copied Adams' software or of "infringement" by the ASUS programs. Adams has reports from third-parties that suggest infringement was a concern, and that ASUS was not the originator of its programs, but these are *suggestions* and are not substantial proof of infringement.

For its part and similarly without any foundation, ASUSTeK simply "denies that it misappropriated Adams' trade secrets or patented technology."[48] "ASUSTeK disputes Plaintiff's unsupported contention that its employee, Sam Yang, relied on or referred to Adams' test programs when developing programs under the names 'ifdc.exe' and 'w2sec.exe.'"[49]

Adams also alleges, without providing evidence, that the ASUS patent application was rejected *because of* Adams' patent. "[T]he USPTO rejected ASUS' patent because Adams had already patented the technology."[50] ASUS disputes this, again without foundation. "ASUSTeK

---

[45] Memorandum in Support at iv (emphasis added).

[46] *Id.* at v (emphasis added).

[47] *Id.* at xii (emphasis added).

[48] Memorandum in Opposition at v.

[49] *Id.* at xi.

[50] Adams' Reply Memorandum in Support of Its Motion for Terminating Sanctions against ASUS (Reply Memorandum) at 3, docket no. 586, filed July 14, 2008. See also Memorandum in Support at xii.

acknowledges that it filed the '367 patent application but this patent application was abandoned. ASUSTek disputes that the US Patent applications make any such connection between these programs and Adams' test programs."[51]

Assertion of Destruction of Evidence

Adams similarly jumps from ASUS' *non-production* of evidence to the conclusion that ASUS has *destroyed* evidence. Adams claims that in spite of numerous discussions of the issues on this motion, "ASUS failed to make any responsive production."[52]

> ASUS has failed and refused to produce FdcCheck.exe, HPFDC.exe, the source code for ifdc.exe, w2sec.exe, the source code for w2sec.exe, w4sec.exe, and the source code for w4sec.exe; and it has failed and refused to produce a single document or email relating to ASUS' development and use of these test programs. Specifically, ASUS has failed and refused any correspondence or related documents whatsoever for those programs or for ASUS' activities with its suppliers (e.g., Winbond) and its customers (e.g., Sony).[53]

It is true that most of the documentation on which Adams relies on this motion was produced by parties other than ASUS. Only the executable "ifdc.exe;" the patent application; and the two Yang emails were produced by ASUS. The two Yang emails were produced months after this motion was filed.

Because ASUS has produced so little, Adams therefore draws the conclusion that ASUS has destroyed evidence.

> ASUS's only response is that it has produced a large volume of documents. That may be the case; but, it has not produced the most critical documents – those that relate to its misappropriation, its copying, and its willful behavior. The only conclusion after all this time is that ASUS has destroyed critical evidence that it simply cannot show did not exist.[54]

---

[51] Memorandum in Opposition at xi.

[52] Memorandum in Support at xiv.

[53] *Id.* at x (emphasis omitted).

[54] *Id.* at xiv.

Adams makes a similar conclusion of destruction as to the source code for the test programs. "ASUS has spoliated the most critical evidence in this case, e.g., test programs and related source code"[55] "[S]ince ASUS has not produced it, the only conclusion is that ASUS has destroyed it."[56]

As expected, ASUSTeK "denies in the strongest terms Plaintiff's allegations it destroyed relevant evidence after being on notice of Plaintiff's claims . . . ."[57] "[N]o documents, programs or source code have been discarded since ASUSTeK received some information of Plaintiff's potential claims against ASUSTeK in early 2005."[58]

ASUS' Data Resources

ASUS extensively describes its email management and storage practices, to explain the nearly complete absence of emails related to the subject of this litigation. First, ASUS says its email servers are not designed for archival purposes, and employees are instructed to locally preserve any emails of long term value.

> 35. ASUSTeK employees send and receive email via company email servers.
>
> 36. Storage on ASUSTeK's email servers is limited, and the company directs employees to download those emails they deem important or necessary to perform their job function from the company email server to their individual company issued computer.
>
> 37. ASUSTeK informs its employees that any email not downloaded to an employee's computer are automatically overwritten to make room for additional email storage on ASUSTeK's servers.
>
> 38. It is ASUSTeK's routine practice that its employees download to their individual computer those emails the employee deems important or necessary to perform his or her job function or comply with legal or statutory obligations.[59]

[55] *Id.* at iv.

[56] *Id.* at xi.

[57] Memorandum in Opposition at v.

[58] *Id.* at x.

[59] *Id.* at xxvi – xxvii.

Second, ASUS employee computers are periodically replaced, at which time ASUS places all archiving responsibility for email *and other documents* on its employees.

> 39. During the course of their employment, ASUSTeK employees return their individual company issued computers in exchange for newer replacement computers.
>
> 40. The hard drives of all computers returned to or exchanged with the company are formatted to erase all electronic information stored on these computers before they are recycled, reused or given to charity.
>
> 41. During a computer exchange, it is ASUSTeK's practice to direct its employees to download those emails and electronic documents from the employee's individual computer to the employee's newly issued computer that the employee deems important or necessary to perform his or her job function or comply with legal or statutory obligations.[60]

These practices may explain why ASUS has not produced certain emails which Adams has received from other parties. However, this information does not establish the good-faith nature of ASUS data management practices. This will be explored later in the discussion of sanctions.

Motions to Strike

ASUS has moved to strike the four emails produced by Winbond, the Woon Report, the printouts of the program headers, and Adams' related arguments.[61] ASUS alleges these documents are not authenticated and are inadmissible hearsay. As to the program header printouts, ASUS also alleges "any probative value of the document is substantially outweighed

[60] *Id.* at xxvi – xxvii.

[61] ASUSTeK's Motion to Strike Exhibit E to Plaintiff's Memorandum in Support of Its Motion for Terminating Sanctions (First Motion to Strike), docket no. 559, filed June 30, 2008; ASUSTeK's Motion to Strike Exhibits A, B, C, D and I and Related Arguments in Plaintiff's Memoranda in Support of Its Motion for Terminating Sanctions against ASUSTeK (Second Motion to Strike), docket no. 604, filed August 21, 2008.

by the danger of unfair prejudice to ASUSTeK, confusion of the issues, and misleading the jury.[62]

Waiver of Motion to Strike Emails and Program Header Printouts

Adams asserts that ASUS' motion to strike the emails and printouts of program headers is untimely because ASUS delayed its motion to strike those items until nearly two months after its other motion to strike which was filed with ASUS' opposition to the motion for sanctions.[63] ASUS claims that no rule sets a deadline for filing a motion to strike.[64] On this point, the court agrees with ASUS and will rule on the motions to strike.

Authentication

ASUS moves to strike exhibits which Adams uses to support the motion for sanctions because the exhibits are not authenticated. The exhibits attacked are the four Winbond emails, the Woon Report and the program header printouts.

As to the Woon Report, ASUS states "Plaintiff has not submitted any declaration from YC Woon authenticating the notes.[65] Further, there is no indication regarding the circumstances of their creation."[66] The Woon Report has, however, been sufficiently authenticated by the deposition of Mike Holstein and emails sent and received near the time of the report which are

---

[62] Second Motion to Strike at 2 (citing Fed. R. Evid. 403, 801(a-c), 802 & 901).

[63] Adams' Opposition to ASUSTeK's Motion to Strike [Dkt. No. 604] Exhibits A, B, C, D and I (Opposition to Second Motion to Strike) at iii, 7-9, docket no. 615, filed September 8, 2008.

[64] Reply in Support of ASUSTeK's Motion to Strike Exhibits A, B, C, D & I and Related Arguments in Plaintiff's Memoranda in Support of Its Motion for Terminating Sanctions at 8-9, docket no. 623, filed September 22, 2008.

[65] ASUS is here using the term "notes" to mean the entire report. The reply memorandum on this motion discusses the typewritten "pages" and handwritten "notes." Reply Memorandum in Support of ASUSTeK's Motion to Strike Exhibit E to Plaintiff's Memorandum in Support of Its Motion for Terminating Sanctions (Reply Memorandum in Support of First Motion to Strike) at 3-7, docket no. 595, filed July 28, 2008.

referenced in that deposition.[67] While Holstein admitted he did not know if Woon personally wrote the report,[68] Holstein did authenticate the typed pages as Woon's report. The report as proffered by Adams consists of typewritten and handwritten pages.[69] For this discussion, and the balance of this order, the handwritten pages are ignored.

As to the emails, ASUS says "Plaintiff has not submitted a sworn testimony that the emails attached as Exhibits A through D to its memorandum are authentic under Fed. R. Evid. 901, which requires a witness with "knowledge ... that a matter is what it is claimed to be."[70] These emails were first produced by Winbond in the Gateway case, not in this case.[71] Winbond was not a party to the Gateway case, but is a party in this case. While it is not clear on this record whether Winbond also produced the emails in this case, it is clear that Winbond would readily authenticate them again by production, which would be an effective authentication against all parties to the case.[72] Authentication for this motion is satisfied.

ASUS also makes an authentication objection to the program header printouts:

> Plaintiff's explanation of the source of [the program header printouts] is 'A copy of each programming header is attached hereto as Exhibit I'. Plaintiff's cursory account of Exhibit I's origin is insufficient under Rule 901, which requires

---

[66] Memorandum in Support of ASUSTeK's Motion to Strike Exhibit E to Plaintiff's Memorandum in Support of its Motion for Terminating Sanctions (Memorandum in Support of First Motion to Strike) at 2, docket no. 560, filed June 30, 2008.

[67] Adams' Supplementation at 4-9. Adams also argued for authenticity of the Woon Report by other means in Adams' Opposition to ASUSTeK's Motion to Strike [Dkt no. 559] Exhibit E to Plaintiff's Memorandum in Support of its Motion for Terminating Sanctions (Opposition to First Motion to Strike), docket no. 584, filed July 14, 2008.

[68] ASUSTeK's Response to Docket No. 675 at 7, docket no. 707, filed under seal January 23, 2009.

[69] Exhibit E to Memorandum in Support.

[70] Memorandum in Support of ASUSTeK's Motion to Strike Exhibits A, B, C, D and I and Related Arguments in Plaintiff's Memoranda in Support of Its Motion for Terminating Sanctions Against ASUSTeK (Memorandum in Support of Second Motion to Strike) at 2, docket no. 609, filed August 21, 2008 (citing Fed. R. Evid. 901(b)(1)).

[71] Opposition to Second Motion to Strike at v-vi and 2.

[72] *Id. Orr v. Bank of Am.*, 285 F.3d 764, 776 (9th Cir. 2002).

> "evidence sufficient to support a finding that the matter in question is what its proponent claims."[73]

Again, the program files were produced by Winbond as having been received from ASUS, so the printouts are sufficiently authenticated for this motion.[74]

Adams notes that ASUS has not repudiated any of the documents, but has only claimed that they are not sufficiently authenticated.[75] In addition, ASUS has not offered any evidence to contradict the emails, Yoon Report or program header printouts. As ASUS argues, "ASUSTeK never claimed 'that there is no evidence' linking programs to its former employee Sam Yang. Rather, ASUSTeK stated that Plaintiff's claim that Sam Yang authored the programs was not properly supported with admissible evidence." [76] At this point, the authentication of the evidence offered by Adams is sufficient in light of ASUS' marginal challenge.

ASUS claims a nearly total absence of evidence, disputing any evidence produced by other parties. The purpose of authentication is to buttress reliability and filter untrustworthy evidence. ASUS is using the requirement of authentication, in conjunction with its internal evidence vacuum, to eliminate the only evidence available because ASUS will not repudiate, authenticate or contradict it. That the evidence comes from other sources will be considered as to the weight the evidence may have, but ASUS should not be able to prevent consideration of the best evidence available, which has reasonable assurances of authenticity.

---

[73] Memorandum in Support of Second Motion to Strike at 2 (quotingMemorandum in Support at xii -xiii).

[74] Opposition to Second Motion to Strike at v; Memorandum in Support at xiii.

[75] Opposition to Second Motion to Strike at 1.

[76] ASUSTeK's Response to Docket No. 675 at 8, docket no. 707, filed under seal January 23, 2009.

Hearsay

ASUS also claims each of the emails, the Woon Report and the program headers are inadmissible hearsay. ASUS objects to the Woon Report because "YC Woon. . . has not offered a declaration or affidavit in this matter. Further, there is no indication regarding the circumstances of their creation."[77] As to the emails interchanged between Winbond employees, ASUS claims that there is no evidence the authors speak for Winbond, much less for ASUS.[78] As to the program header printouts, ASUS objects that Adams has no evidence that "the programs were authored, sent or received by or from ASUSTeK."[79]

Woon Report

Adams argues that the Woon Report is admissible hearsay under the business records exception[80] and as a non-hearsay admission of a party opponent.[81]

The Woon Report contains statements which would be adverse to the interests of ASUS, but no source is given for these statements.

> Apparently the utility's algorithm originated from one of IBM's consulting firm. [sic] ASUS wrote software using the same algorithm and use it to test the boards in ASUS. As this is a propriety software, and also due to its patented algorithm, the software could not be released to be used outside of ASUS. Winbond apparently got hold of the software through ASUS as they bought the same Winbond chip from them.[82]

---

[77] Memorandum in Support of First Motion to Strike at 3.

[78] Memorandum in Support of Second Motion to Strike at 3-5.

[79] *Id.* at 6.

[80] Opposition to First Motion to Strike at 9 (citing Fed. R. Evid. 803(6)).

[81] *Id.* at 9, 11 (citing Fed. R. Evid. 801(d)(2)(D)).

[82] Woon Report.

The report itself has no indication that a representative of ASUS was present on July 31, 2000, during events reported.[83] An admission must be made "by the party's agent or servant concerning a matter within the scope of the agency or employment . . . ."[84] The Woon Report is authored by a *Gateway* employee, and has not been shown to contain a statement of a person authorized to speak for ASUS,[85] so it is not a non-hearsay admission.

But the report is a business record, in spite of ASUS' arguments that Woon was on "special assignment."[86] Such trips and events are regular business activity and reports are regularly made. The emails surrounding the date of the report show that Woon's activities were regularly recorded and reported.[87] Woon was reporting to others in Gateway on central business issues, so it can be presumed he had a duty to report accurately. Indeed, this is apparent from the detail in the report. And the typewritten report was created and emailed the same day as the events reported.[88] Fed. R. Evid. 803(6) is satisfied.[89]

However, the critical statements are not Woon's observations of events, but his reporting of statements of unidentified persons.

> *Apparently* the utility's algorithm originated from one of IBM's consulting firm [sic]. ASUS wrote software using the same algorithm and use it to test the boards in ASUS. As this is a proprietary software, and also due to it's [sic] patented

---

[83] Reply Memorandum in Support of First Motion to Strike at 9.

[84] Fed. R. Evid. 801(d)(2)(D).

[85] Reply Memorandum in Support of First Motion to Strike at 7-8.

[86] *Id.* at 8.

[87] Exhibit 28 to the Deposition of Mike Holstein, December 19, 2008, attached as Exhibit 3 to Adams' Supplementation.

[88] *Id.*

[89] (6) Records of regularly conducted activity. A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record or data compilation, all as shown by the testimony of the custodian or other qualified witness . . . unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness.

> algorithm, the software could not be released to be used outside of ASUS. Winbond *apparently* got hold of the software through ASUS as they bought the same Winbond chip from them. [90]

As ASUS argues, these are "conclusory statements" without identifying the unknown declarant(s), and without providing foundation for the declarants' alleged statements."[91] The Woon Report is admissible hearsay as to what Woon reported and observed, but these specific statements are double hearsay.[92] On the current state of the record, there is insufficient foundation to establish a second hearsay exception, to give the "guarantees of trustworthiness"[93] that would enable these statements to be used against ASUS on this motion.

Winbond Emails

The Winbond emails are admissible business records of Winbond. They reflect the activities and knowledge of Winbond and only mention involvement of ASUS. The emails do not contain conclusive statements similar to those in the Woon Report. Because the records themselves are the actual communications, they are timely recorded, regular activities; they memorialize events and conditions; and they have no indicia of untrustworthiness. They do not purport to reflect statements of unidentified third parties. ASUS objects to them because they may be offered for truthfulness of the statements contained in them. For example, ASUS asserts that in the first email "Plaintiff attempts to characterize an alleged FDC error as 'Life or Death' for the entire computer industry."[94] That "Life or Death" statement, like other statements in the emails is a statement of Winbond's perception. No one claims Winbond speaks for the industry.

---

[90] Woon Report (emphasis added).

[91] Reply Memorandum in Support of First Motion to Strike at 10.

[92] Fed. R. Evid. 805.

[93] Advisory Committee Notes to Federal Rules of Evidence, Art. III, Hearsay.

[94] Memorandum in Support of Second Motion to Strike at 3.

ASUS claims that in the third email, there is content that might be taken as a statement from ASUS. "[W]e are informed by Asus that it does happen in our W83877TF [chip]."[95] ASUS' objection to the second email is similar. These statements must be taken as Winbond's perception and understanding. ASUS has offered nothing to indicate the information in these emails is untrustworthy.

Objecting to the fourth email, ASUS seems to protest too much. ASUS asserts that the statement "The US 5739414 patent has claim [sic] this similar solution" tends to show "that ASUSTeK knew the 'solution' discovered was 'similar' to some unspecified part of the '414 patent."[96] Nothing in that email mentions ASUS. The statement can only be read as Winbond's understanding.

The double hearsay problem found in the Woon Report does not exist in the Winbond emails, because they are statements of Winbond's activities, and while they reflect interaction with ASUS, they are written to record Winbond's perceptions, reactions and plans. The Woon Report, by contrast, makes significant unsourced conclusions. The emails, internal to Winbond, are not like the Woon Report of inter-company contact.

Program Headers

Exhibit I is offered to buttress the connection of Sam Yang and ASUS to the programs ifdc.exe and w4sec.exe. After the original briefing on this motion, ASUS has provided emails from Sam Yang which reference and enclose those programs.[97] While these programs were not

---

[95] *Id.* at 4.

[96] *Id.* at 5.

[97] Email January 27, 2000 9:18 am, Sam Yang to Max Lu, attached as Exhibit 1 and email January 27, 2000 1:26 pm, Sam Yang to Max Lu, attached as Exhibit 2 to Adams' Supplementation. Before producing those emails, ASUS took the position "that Plaintiff's assertion that ASUSTeK created ifdc.exe and w2sec.exe is supported only by unauthenticated notes and hearsay of another party." Memorandum in Opposition at viii.

produced with the emails and were produced by Winbond, not ASUS, they were produced by Winbond as having come from ASUS.[98] Coupled with the emails, the program header printouts constitute admissible business records. The arguments ASUS makes about authenticity and chain of custody all go to weight.[99]

Confusion and Prejudice – Program Headers

ASUS points out that the printout of the program headers is largely unintelligible,[100] and claims that Adams unjustifiably argues the printout proves much more than the document states.[101]

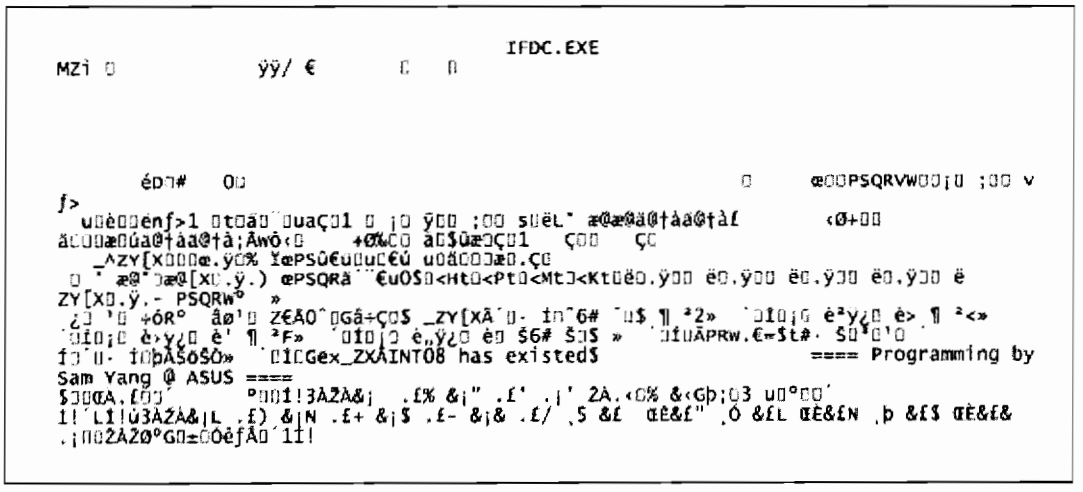
> The only legible text in Exhibit I includes the following: "IFDC.EXE," "has existed" and "Programming by Sam Yang @ ASUS" on the first page and "W4SEC.EXE" and "Programming by Sam Yang @ ASUS" on the second page. Plaintiff alleges that "IFDC.EXE," "W4SEC.EXE" and "Programming by Sam Yang @ ASUS" proves that Sam Yang, a former ASUSTeK employee, created programs labeled IFDC.EXE and W4SEC.EXE in Plaintiff's possession by copying Plaintiff's "patented algorithm."

---

[98] Memorandum in Support at xii.

[99] Memorandum in Support of Second Motion to Strike at 6.

[100] For example, the first page of the ifdc.exe program header printout is reproduced below:



IFDC.EXE

MZi □ ÿÿ/ € □ □

éD¬# 0□ □ œ□□PSQRVW□□¡□ ;□□ v

ƒ>

u□è□□enf>1 □t□ä□¨□uaÇ□1 □ ¡□ ÿ□□ ;□□ s□ëL˙ æ@æ@ä@†àä@†àf ‹Ø+□□

ä□□□æ□úä@†àä@†à;ÄwÓ‹□ +Ø‰□□ à□$□æ□Ç□1 Ç□□ Ç□

_^ZY[X□□□œ.ÿ□% ŁœPS□€u□u□€ú u□ä□□□æ□.Ç□

□ ˙ æ@˙□æ@[X□.ÿ.) œPSQRä ¨€uO$□<Ht□<Pt□<Mt□<Kt□ëD.ÿ□□ ë□.ÿ□□ ë□.ÿ□□ ë□.ÿ□□ ë

ZY[X□.ÿ.- PSQRw° »

¿□ '□ +óR° åø'□ Z€Ä0ˆ□Gâ÷Ç□$ _ZY[XÄ´□· ín¯6# ¯u$ ¶ ²2» ¨□Í□¡□ è²y¿□ è› ¶ ²<»

¨□Í□¡□ è›y¿□ è' ¶ ²F» ´□Í□¡□ è„ÿ¿□ è□ $6# Š□$ » ´□íuÄPRw.€=$t#· Š□¶□'□ ˙

f□´□· í□þÄŠöŠÖ» ¨□Í□Gex_ZXÄINT08 has existed$ ==== Programming by

Sam Yang @ ASUS ====

$□□ŒA.£□□´ ³□□1!3ÀŽÀ&¡ .£% &¡" .£' .¡' 2À.‹□% &‹G þ;□3 u□°□□´

1!´L1¡ú3ÀŽÀ&¡L .£) &¡N .£+ &¡$.£- &¡& .£/ ¸5 &£ Œ£&£" ¸Ó &£L Œ£&£N ¸þ &£$ Œ£&£&

.¡□□2ÀŽØ°G□±□Ò¢fÂ□´11!

[101] Memorandum in Support of Second Motion to Strike at 7.

Adams responds that "the text that is legible is certainly probative: it links Sam Yang, a former engineer at ASUS, to test programs misappropriating Adams' technology" and that since a judge, not a jury is deciding this motion, "the argument of unfair prejudice carries little weight."[102] Adams is correct. Computer gobblydegook is not confusing or prejudicial.

Summary of Remaining Evidence on this Motion

Adams' evidence that the magistrate judge is considering on this motion includes:

- Sam Yang emails dated January 27, 2000 which enclosed programs ifdc.exe, w4sec.exe and w2sec.exe;
- Programs ifdc.exe, w4sec.exe produced by Winbond as having come from ASUS which have "Programming by Sam Yang@ASUS" in the headers;
- The application for patent application for "preventing data corruption by a floppy diskette controller" by ASUS/Sam Yang filed October 15, 2001;
- Winbond emails dated January 27, 31 and February 8, 2000, regarding floppy disk controller issues to show that:
    - Winbond regarded the issue as "'LIFE-OR-DEATH' to the I/O business;"
    - Winbond reported that ASUS had special software related to the issue;
    - Winbond believed the '414 patent had a "similar solution" and Winbond was concerned about infringement; and
    - Winbond had heard that HP representatives were visiting ASUS and HP and ASUS representatives were working together.

These specific facts are in an undisputed context, though the parties disagree on the significance of these contextual facts. The Toshiba class action was settled in October 1999. Other class actions were then pending. Thereafter, other computer and component manufacturers made significant inquiries into the floppy disk controller error issue. Adams has

[102] Opposition to Second Motion to Strike at 7.

been involved in some suits and settlements with these manufacturers, and most of that activity commenced in the 2000 timeframe.

In presentation of argument on this motion the only documents ASUS has produced regarding the development of its floppy disk controller test software are the two Sam Yang emails (produced after the filing of this motion) and an executable copy of ifdc.exe. ASUS has explained that it has no centralized storage of electronic documents, email or otherwise, and relies on individual employees to archive email (which will be deleted if left on the server) and electronic documents (which reside only on individual workstations). ASUS has separately stated that Yang currently recalls writing programs regarding floppy disk controller errors;[103] that the second Winbond email evidences ASUSTeK's regular work with Winbond;[104] and that the fourth email shows "good faith efforts to avoid infringement."[105]

[103] Declaration of Vincent Hong, docket no. 556, filed June 30, 2008.

[104] Memorandum in Opposition at v.

[105] *Id.* at v.

Motion for Sanctions

The threshold issues on a spoliation motion include establishing (a) that evidence has been lost, destroyed or made unavailable and (b) that the party against whom sanctions are sought had a duty to preserve the evidence. If those facts are shown, the determination of sanctions is subject to other standards.

Unavailable Evidence

Adams recites a list of materials ASUS would be expected to have, based on the facts before the court on this motion:

(1) the ASUS test programs' source code and documentation of their development;

(2) documentation of ASUS' FDC and motherboard testing activities in the 2000-2001 time period;

(3) ASUS' communications with suppliers regarding testing of the FDC problems;

(4) ASUS' communications with design experts relating to Adams' technology; and

(5) documentation of discussions occurring internally within ASUS regarding whether to license Adams' technology.[106]

In addition, ASUS would be expected to have communications with its customers about the FDC error issue; efforts to resolve the issue; and documentation of its patent application process for its detector technology.

Adams claims that "[t]he evidence that Winbond provided in the Gateway litigation does not leave any doubt that these documents existed and that ASUS had them."[107] Certainly, other parties have provided evidence that one would expect ASUS to have as well. And the volume

[106] Memorandum in Support at 3-4.

[107] *Id.* at xiii.

and tenor of the Winbond communication and concurrent Yang emails would suggest ASUS should have far more evidence than it has produced in this case.

ASUS' own statements and productions highlight data that is missing. "[N]o documents, programs or source code have been discarded since ASUSTeK received some information of Plaintiff's potential claims against ASUSTeK in early 2005."[108] ASUS therefore admits that materials prior to 2005 could have been destroyed because of its information management practices. ASUS has produced a CD with program files from the time at issue, [109] but somehow the ASUS source code at issue in this case was not available.

ASUS contacted each of the current employees identified by Adams as potentially aware of floppy disk controller errors in the pertinent timeframe; has interviewed them; and asked them to search their company-issued computers for related data.[110] Most of them did not work on floppy disk controller errors, and "any documents from the 1999-2002 time period were discarded prior to early 2005 . . . pursuant to the company's routine practice of discarding unnecessary documents and information."[111]

The only former employee that ASUS describes contacting is Sam Yang, presumably because ASUS says "ASUSTeK is unaware of any employee who worked on the floppy disk controller overrun/under-run matters other than engineer Sam Yang."[112] But without asking those other former employees, it is not possible to be certain they did not work on the project.

---

[108] Memorandum in Opposition at x.

[109] *Id.* at xix.

[110] *Id.* at xxx-xxxi.

[111] *Id.* at xxxi.

[112] *Id.* at xxxii.

So, due to ASUS' lack of inquiry we have no evidence from most of the former ASUS employees.

ASUS has had contact with former employee Sam Yang,[113] but Adams' counsel's attempts to contact him have been frustrated.[114] Therefore Adams has nothing from the most central character in ASUS' work

Duty to Preserve

The universe of materials we are missing is very large. Indisputably, we have very little evidence compared to what would be expected. The next issue is ASUS' duty to preserve evidence, and whether the lack of evidence is due to breach of that duty. ASUS claims that its duty to preserve documents related to these claims arose only in early 2005.

Adams' Notice to ASUS

In ASUS' own words,

> ASUSTeK's retention of documents relating to the subject matter of this litigation and patents-in-suit has been influenced by the timing of Plaintiff's notice to ASUSTeK.[115]
>
> On February 23, 2005, ASUSTeK first became aware that Plaintiff may assert a claim for patent infringement against ASUSTeK under the 002 Patent as a result of a letter . . . delivered to ASUSTeK by Plaintiff's counsel . . . .[116]

While Adams' counsel wrote an earlier letter to ASUS, which was attached to the February 2005 letter ASUS says it "has no record of receiving that certain letter dated October 4, 2004 from Phillips to ASUSTeK . . . .[117] With a benchmark date of February 23, 2005, ASUS

---

[113] Declaration of Vincent Hong at 5-8, docket no. 556, filed June 30, 2008.

[114] Opposition to Second Motion to Strike at vi.

[115] Memorandum in Opposition at 44.

[116] *Id.* at xviii

[117] *Id.* at xix

claims it has fully complied with its duties to preserve documents. "Since February 23, 2005, when Plaintiff first notified ASUSTeK of potential infringement claims, ASUSTeK has not destroyed any evidence relevant to such claims."[118]

Adams' Delay

ASUS claims that Adams' delay in giving notice and bringing suit is the reason it has so little documentation. "ASUSTeK's ability to locate and produce documents from 2000/2001 has been significantly inhibited by Plaintiff's delay in informing ASUSTeK of potential claims against ASUSTeK, and because of Plaintiff's continued failure to identify any infringing devices."[119] ASUS alleges that this delay works to its prejudice rather than merely to prejudice Adams.

> Given the passage of time from 2000 to May of 2007, and Plaintiff's delay in filing suit once it discovered the alleged infringing behavior and technology of the parties, ASUSTeK [will] likely suffer significant evidentiary prejudice due to faded memories, the inability to locate key witnesses, and the loss or inability to locate allegedly relevant records in this case.[120]

When Did the Duty To Preserve Arise?

Adams and ASUS agree that a litigant's duty to preserve evidence arises when "he knows or should know [it] is relevant to imminent or ongoing litigation."[121] ASUS' arguments pin this date to the first letter from Plaintiff's counsel. However, counsel's letter is not the inviolable benchmark. In *103 Investors I, L.P. v. Square D Co.,*[122] the plaintiff building owner sued an electrical parts manufacturer for failure to warn of proper care for a part alleged to have been the

---

[118] *Id.* at 3-4.

[119] *Id.* at xiv.

[120] *Id.* at 5-6.

[121] *Jordan F. Miller Corp. v. Mid-Continent Aircraft Service, Inc.*, No. 97-5089, 1998 WL 68879, *5 (10th Cir. Feb. 20, 1998).

[122] 470 F.3d 985 (10th Cir. 2006).

fire ignition point. "[A]fter the fire . . . without notice to the defendant [manufacturer], plaintiff threw away fifty to sixty feet of the busway and saved only four feet. The portion of the busway that was saved was not a piece that would have contained a warning [label]."[123] The disposition of the busway was long before suit was filed. But "[t]he district court found that plaintiff had a duty to preserve the evidence because it knew or should have known that litigation was imminent. . . ."[124]

In late 1999, Toshiba paid billions of dollars in a class action settlement related to the floppy disk errors at issue[125] and a class action lawsuit was filed against HP.[126] In early 2000, Sam Yang was writing emails about his work on the software ASUS was using "to verify the FDC write-data distortion."[127] In late 2001, a patent application was filed by Yang and ASUS.[128] In April 2000 a class action lawsuit was filed against Sony based on this alleged defect.[129] Throughout this entire time, computer and component manufacturers were sensitized to the issue. The time period was the technology equivalent of the *103 Investors'* building fire. The building owner may not have known that a defective wiring bus caused the fire, or that suit would be filed, but the owner had a duty to preserve immediately after the fire. In the 1999-2000 environment, ASUS should have been preserving evidence related to floppy disk controller errors.

---

[123] *Id.* at 988.

[124] *Id.* at 989.

[125] Memorandum in Support at iv.

[126] Reply Memorandum at 6-7.

[127] Email January 27, 2000 9:18 am, Sam Yang to Max Lu, attached as Exhibit 1 to Adams' Supplementation.

[128] Exhibit G to Memorandum in Support.

[129] Reply Memorandum at 7.

Separate and apart from the benchmark date to *start* preservation is the last date on which information related to the patent application, including the source code, should have been available. Adams says "ASUS would have to have kept the source code for the test programs because its application remained pending until June 2005."[130] ASUS does not explain how, why or when its source code was discarded.

Safe Harbor

ASUS claims it can find a safe harbor against sanctions because of the recently adopted rule that sanctions may not be generally imposed for "failing to provide electronically stored information lost" if a party can show the loss was "a result of the routine, good-faith operation of an electronic information system."[131] First of all, this provision only applies to electronic evidence. ASUS' arguments and factual summaries are very short on any discussion of paper documents. Other than the patent application and the executable file, it does not appear ASUS has produced any significant tangible discovery on the topics where information is conspicuously lacking.

As to the electronic discovery, including email, ASUS provided an extensive declaration from an experienced consultant in e-discovery.[132] While he stated the reasons for and history of ASUS' "distributed information architecture," he did not state any opinion as to the reasonableness or good-faith in the system's operation.[133] And while he says "ASUSTeK's data

---

[130] *Id.* at 4.

[131] Fed. R. Civ. P. 37(e).

[132] Declaration of Allen L. Gurney in Support of Third Party Defendants ASUSTeK Computer, Inc., and ASUS Computer International's Statement of Compliance with Court Order (Declaration of Allen Gurney), docket no. 461, filed February 21, 2008.

[133] *Id.* at 13-14.

architecture relies predominantly on storage on individual user's workstations,"[134] his 31-page declaration does not show he is familiar with the precise practices pointed out in the declarations of employees. Those employees' declarations describe the practice of ASUS' email system to overwrite old data regardless of its significance; ASUS' reliance on employees for all email and data archiving; and the process of replacement of computers, which also relies on employees to transfer data from their old to their new computers.[135] Neither the expert nor ASUS speak of archiving "policies;" they speak of archiving "practices."[136] Apart from archiving, neither the expert nor the employees describe any sort of backup system or data backup policy, past or present. Presumably ASUS' current data is at the mercy of individual employees' backup practices.

The expert does not evaluate risk of data loss from ASUS' reliance on employees though he does specifically mention the expected turnover of employees in this industry[137] which would seem to heighten the risk. He does mention that certain financial-related data is stored in centrally accessible and presumably secure, backed-up servers.[138] ASUS does know how to protect data it regards as important.

The information before the court does not demonstrate that ASUS' loss of electronic information is within the safe harbor provision. Further, there has been no explanation of the loss of other information.

---

[134] *Id.* at 13.

[135] Memorandum in Opposition at xxvi – xxvii.

[136] *Id.* at xxxi; Declaration of Allen Gurney at 6.

[137] Declaration of Allen Gurney at 14.

[138] *Id.*

What Sanction is Appropriate?

"When deciding whether to sanction a party for the spoliation of evidence, courts have considered a variety of factors, two of which generally carry the most weight: (1) the degree of culpability of the party who lost or destroyed the evidence, and (2) the degree of actual prejudice to the other party."[139] The most widely known sanction is the adverse inference instruction, but other sanctions range from admonitions to granting judgment or dismissal.

Culpability

In the Tenth Circuit, "the general rule is that bad faith destruction of a document relevant to proof of an issue at trial gives rise to an inference that production of the document would have been unfavorable to the party responsible for its destruction."[140] However, "[c]ourts have not generally imposed a similar requirement of bad faith when considering other sanctions for the spoliation of evidence . . . ."[141] The culpability of a party is a signficant factor, but not determinative. Culpability may not mean evil intent, but may simply signify responsibility and control.

A sliding scale of sanctions may be imposed depending on the degree of control the alleged spoliator had over the evidence and the spoliator's subjective intentions. Case law defines the factors to consider when terminating sanctions are sought.

> The district court should consider the following factors when considering whether dismissal is an appropriate sanction: (1) the degree of actual prejudice to the opposing party, (2) the degree of interference with the judicial process, (3) the litigant's culpability, (4) whether the litigant was warned in advance that dismissal was a likely sanction, and (5) whether a lesser sanction would be effective.[142]

---

[139] *Jordan Miller,* 1998 WL 68879, at *4.

[140] *Aramburu v. Boeing Co.,* 112 F.3d 1398, 1407 (10th Cir. 1997).

[141] *Jordan Miller,* 1998 WL 68879, at *4.

[142] *LaFleur v. Teen Help,* 342 F.3d 1145, 1151 (10th Cir. 2003).

In this case, ASUS has not been warned of the possibility of a terminating sanction, and has not been subject to prior orders regarding discovery conduct. Because Adams does have some other sources for evidence, it is likely that a terminating sanction will not be appropriate.

The culpability in this case appears at this time to be founded in ASUS' questionable information management practices. A court – and more importantly, a litigant – is not required to simply accept whatever information management practices a party may have. A practice may be unreasonable, given responsibilities to third parties. While a party may design its information management practices to suit its business purposes, one of those business purposes must be accountability to third parties.

For example, a recreation park's policy to destroy records at the end of each season – prior to the running of the applicable statute of limitations for injuries – has been held to entitle the plaintiff to an adverse inference instruction.[143] In another case where an indexing system made documents practically inaccessible, the court spoke of a party's duty to use an adequate information management system:

> [U]tilizing a system of record-keeping which conceals rather than discloses relevant records, or makes it unduly difficult to identify or locate them, [renders] the production of the documents an excessively burdensome and costly expedition. To allow a defendant whose business generates massive records to frustrate discovery by creating an inadequate filing system, and then claiming undue burden, would defeat the purposes of the discovery rules. [144]

Similarly, here, ASUS' system architecture of questionable reliability which has evolved rather than been planned, operates to deny Adams access to evidence. This should not be excused.

---

[143] *Reingold v. Wet 'N Wild Nevada Inc.*, 944 P.2d 800 (Nev. 1997), overruled on other grounds by *Bass-Davis v. Davis*, 134 P.3d 103 (Nev. 2006).

[144] *Kozlowski v. Sears, Roebuck*, 73 F.R.D. 73 (D. Mass. 1976).

ASUS did not have a designed information management policy taking varying needs into account. ASUS offers no statements from management-level persons explaining its practices, or existence of any policies.

"An organization should have reasonable policies and procedures for managing its information and records."[145] "The absence of a coherent document retention policy" is a pertinent factor to consider when evaluating sanctions.[146] Information management policies are not a dark or novel art. Numerous authoritative organizations have long promulgated policy guidelines for document retention and destruction.

> Organizations issuing guidance in this area include ANSI (American National Standards Institute), AIIM (Association for Information and Image Management), ARMA International (Association of Records Managers and Administrators) and ISO (International Organization for Standardization).
> In 2001, ISO sought an international consensus standard for records management, including electronic records, in its guidance document ISO Technical Report 15489-2 (*Information and Documentation—Records Management* (2001)) and its accompanying standard, ISO 15489-1.16.[147]

ASUS' practices invite the abuse of rights of others, because the practices tend toward loss of data. The practices place operations-level employees in the position of deciding what information is relevant to the enterprise and its data retention needs. ASUS alone bears responsibility for the absence of evidence it would be expected to possess. While Adams has not shown ASUS mounted a destructive effort aimed at evidence affecting Adams or at evidence of ASUS' wrongful use of intellectual property, it is clear that ASUS' lack of a retention policy and irresponsible data retention practices are responsible for the loss of significant data.

---

[145] Guideline 1, The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age (November 2007).

[146] Telectron, Inc. v. Overhead Door Corp. 116 F.R.D. 107, 123 (S.D. Fla. 1987)

[147] The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age (November 2007).

Prejudice

Prejudice might be considerable. The evidentiary barriers ASUS asserts to the use of documents produced by third parties, and the apparent unavailability of Yang, the only person ASUS says worked on floppy disk controller error detection, combine to show that prejudice is substantial.

In many cases, terminating sanctions have been imposed against a party because its actions made evidence unavailable. Cases have been dismissed against Plaintiffs who caused evidence to be unavailable when:

- a car was destroyed before suit was filed,[148]
- a space heater was discarded two years before filing suit,[149]
- a truck trailer was disposed of as wreckage two months before suit was filed after saving the allegedly defective part,[150]
- parts of a gas grill were discarded two years before litigation,[151] and
- a vehicle was sold for salvage three years before litigation.[152]

At least one jurisdiction has a rule that a product liability case alleging a defect in the specific item and not in the run of production must be dismissed if the product is unavailable for a reason attributable to the plaintiff, even if the destruction is inadvertent.[153] When it is a defendant who has made evidence unavailable, default judgment may be entered.[154] In these

---

[148] *Dillon v. Nissan Motor Co.*, 986 F.2d 263 (8th Cir. 1993).

[149] *Unigard Security Ins. Co. v. Lakewood Eng. & Mfg. Corp.*, 982 F.2d 363, 367 (9th Cir. 1992)(citing two other cases imposing sanctions for pre-filing destruction of evidence).

[150] *Stubli v. Big D Int'l Trucks, Inc.*, 810 P.2d 785 (Nev. 1991).

[151] *Allstate Ins. Co. v. Sunbeam Corp.*, 53 F.3d 804 (7th Cir. 1995).

[152] *Silvestri v. General Motors Corp.*, 271 F.3d 583 (4th Cir. 2001).

[153] *Lee v. Boyle-Midway Household Prods, Inc.*, 792 F. Supp. 1001, 1005-06 (W.D. Pa. 1992) *(citing Roselli v. General Elec. Co.*, 410 Pa.Super. 223 (Pa.Super. 1991)).

[154] *Computer Associates Intern., Inc. v. American Fundware, Inc.*, 133 F.R.D. 166, 171 (D.Colo. 1990).

cases the prejudice was so severe as to deny justice in court. Spoliation remedies are intended to compensate for the partial or total loss of the ability to litigate.

Prejudice by loss of evidence must be measured in light of "other evidence available."[155] These motions were briefed months ago. Even now, fact discovery related to Adams' claims is still open. It is scheduled to close May 15, 2009.[156] Therefore the degree of prejudice and the appropriate sanction cannot be determined until the close of discovery. Adams and ASUS will be directed to provide further briefing to enable determination of prejudice and the appropriate sanction.

ORDER

IT IS HEREBY ORDERED that the motion for sanctions[157] is GRANTED IN PART. The magistrate judge finds that ASUS has violated its duty to preserve information and that subject to determination of prejudice, a sanction is appropriate. Fourteen calendar days after the close of fact discovery, ASUS shall provide the court with a summary listing and a copy of all evidence ASUS has produced to Adams of:

(1) the ASUS test programs' source code;

(2) ASUS FDC error test program development;

(3) ASUS' FDC and motherboard testing activities in the 2000-2001 time period;

(4) ASUS' communications with suppliers regarding testing of the FDC problems;

(5) ASUS' communications with design experts relating to Adams' technology;

---

[155] *North v. Ford Motor Co.*, 505 F. Supp. 2d 1113, 1116 (D. Utah 2007).

[156] Order Granting Stipulated Motion to Amend and Amended Scheduling Order, docket no. 728, filed March 24, 2009.

[157] Adams' Motion for Terminating Sanctions Against ASUS Based upon ASUS' Spoliation of Evidence of Its Piracy, docket no. 492, filed April 17, 2008.

(6) discussions occurring internally within ASUS regarding whether to license Adams' technology.

(7) ASUS' communications with its customers about the FDC issue,

(8) ASUS' efforts to resolve the FDC issue; and

(9) ASUS' patent application process for its detector technology.

Fourteen calendar days thereafter Adams may file a response which may also identify all information Adams has received from sources other than ASUS on the above topics which Adams believes would be of evidentiary value in Adams' claims against ASUS, and Adams' specific recommendation for the form of an appropriate sanction. Seven calendar days thereafter, ASUS may reply.

IT IS FURTHER ORDERED that the motion to strike Exhibit E[158] to Adams' memorandum is GRANTED IN PART.

IT IS FURTHER ORDERED that the motion to strike Exhibits A-D and I[159] is DENIED.

March 27, 2009.

Magistrate Judge David Nuffer

[158] ASUSTeK's Motion to Strike Exhibit E to Plaintiff's Memorandum in Support of Its Motion for Terminating Sanctions, docket no. 559, filed June 30, 2008.

[159] ASUSTeK's Motion to Strike Exhibits A, B, C, D and I and Related Arguments in Plaintiff's Memoranda in Support of Its Motion for Terminating Sanctions against ASUSTeK, docket no. 604, filed August 21, 2008.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

JACK R. LORRAINE AND,	**:**	
BEVERLY MACK	**:**	
Plaintiffs	**:**	
	:	
v.	**:**	**CIVIL ACTION NO. PWG-06-1893**
	:	
MARKEL AMERICAN	**:**	
INSURANCE COMPANY	**:**	
Defendants	**:**	

...o0o...

MEMORANDUM OPINION

Plaintiffs/ Counter-Defendants Jack Lorraine and Beverly Mack bring this action to enforce a private arbitrator's award finding that certain damage to their yacht, *Chessie,* was caused by a lightning strike that occurred on May 17, 2004, while *Chessie* was anchored in the Chesapeake Bay.[1] Defendant/ Counter-Plaintiff Markel American Insurance Company ("Markel") likewise has counterclaimed to enforce the arbitrator's award, which, in addition to concluding that certain damage to *Chessie*'s hull was caused by lightning, also concluded that the damage incurred was limited to an amount of $14,100, plus incidental costs. Following discovery, Plaintiffs moved for summary judgment (Paper No. 16), and Defendants filed a response in opposition and cross motion for summary judgment (Paper No. 19), to which Plaintiffs filed an opposition and reply (Paper No. 21), followed by Defendant's reply (Paper No. 23). In a letter order dated February 7, 2007 (Paper No. 26), I denied without prejudice both motions for the reasons discussed more fully below, and informed the parties that I intended to file a more comprehensive opinion explaining my ruling,

[1]This case has been referred to me for all proceedings with the consent of the parties. 28 U.S.C. § 636(c)(1)(2006); Local Rule 301.4.

which is found herein.

BACKGROUND

It is difficult for the Court to provide the appropriate background to the underlying arbitration in this case because, as will be discussed in greater detail below, neither party has proffered any admissible evidence to support the facts set forth in their respective motions. *See* FED. R. CIV. P. 56(c). Based on the pleadings, however, it appears undisputed that *Chessie* was struck by lightning on May 17, 2004, and that Plaintiffs filed a claim with Markel, their insurance carrier, for certain damage incurred as a result of the strike. Compl.¶¶ 5, 6; Answer ¶¶ 2, 6. Markel issued payment under the policy for some of the damage claimed, and the matter would have been concluded had Plaintiffs not discovered damage to the hull when they pulled the boat out of the water several months later. Compl. ¶ 7. Markel denied that the hull damage was caused by the lightning strike and/or covered by Plaintiffs' insurance policy, and initiated a declaratory judgment action in the United States District Court for the Middle District of Pennsylvania to that effect. Compl. ¶ 13, Answer ¶ 15. The parties subsequently negotiated a private arbitration agreement and voluntarily dismissed the Pennsylvania claim. Compl. ¶ 15, Answer ¶ 17.

The scope of the arbitration agreement is the basis of this litigation. The final agreement states, in relevant part,

> The parties to this dispute . . . have agreed that an arbitrator shall determine whether certain bottom damage in the amount of $36,000, to the Yacht CHESSIE was caused by the lightning strike occurring on May 17, 2004, or osmosis, as claimed by [Markel].

Pl.'s Mot. Ex. A, Def.'s Mot. Ex. C. The agreement also contemplated that the arbitrator would issue an "award" within 30 days of the final submission of evidence. *Id*. The arbitrator issued his award

on June 12, 2006. In it, he held that some, but not all, of *Chessie*'s hull damage was caused by lightning. Specifically, the arbitrator stated,

> I find that there *is* a basis for an argument regarding loss related damage. Evidence shows that the lightning strike on Mary 17, 2004 was discharged through the hull below the water line . . . . The **corruption** of the **surface laminate of the bottom** *is* basis for a loss related award . . . . The award amount must be kept in proportion to the ***loss related damage*** only. I find that the repairs relating to that damage should be based on a cost of $300.00 per foot ($14,000.00). Other expenses relating to charges for hauling, mast un-stepping/re-stepping, blocking, storage, moving, launching or environmental fees should be added to that amount.

Def.'s Mot. Ex. D. This award forms the basis for the present litigation, in which both parties ostensibly seek to confirm and enforce the arbitrator's decision.

SUMMARY JUDGMENT STANDARD

Summary judgment is appropriate when there exists no genuine issue as to any material fact and a decision may be rendered as a matter of law. Fed. R. Civ. P. 56(c); *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 247 (1986). The party moving for summary judgment has the burden of demonstrating that there are no genuine issues of material facts to resolve. *Pulliam Inv. Co. v. Cameo Properties*, 810 F.2d 1282, 1286 (4th Cir. 1987). In determining whether summary judgment should be granted, the court "must assess the documentary materials submitted by the parties in the light most favorable to the nonmoving party." *Id.* (citing *Gill v. Rollins Protective Services Co.*, 773 F.2d 592, 598 (4th Cir. 1985)).

If the party seeking summary judgment demonstrates that there is no evidence to support the nonmoving party's case, the burden shifts to the nonmoving party to identify specific facts showing that there is a genuine issue for trial. The existence of only a "scintilla of evidence" is not enough to defeat a motion for summary judgment. Instead, the evidentiary materials submitted must show

facts from which the finder of fact reasonably could find for the party opposing summary judgment. *Anderson,* 477 U.S. at 251.

Moreover, to be entitled to consideration on summary judgment, the evidence supporting the facts set forth by the parties must be such as would be admissible in evidence. *See* FED. R. CIV. P. 56(c); *see also Sakaria v. Trans World Airlines,* 8 F.3d 164, 171 (4th Cir. 1993) (finding that the district court properly did not consider inadmissible hearsay in an affidavit filed with motion for summary judgment); *Mitchell v. Data General Corp.*, 12 F.3d 1310, 1315-16 (4th Cir. 1993) ("The summary judgment inquiry thus scrutinizes the plaintiff's case to determine whether the plaintiff has proffered sufficient proof in the form of admissible evidence that could carry the burden of proof in his claim at trial."). With regard to documentary evidence, this Court previously has held that,

> [u]nsworn, unauthenticated documents cannot be considered on a motion for summary judgment. To be admissible at the summary judgment stage, documents must be authenticated by and attached to an affidavit that meets the requirements of Rule 56(e)-that the documents be admissible in evidence.

Miskin v. Baxter Healthcare Corp. et al., 107 F. Supp. 2d 669 (D. Md. 1999) (Grimm, J.) (citing *Orsi v. Kirkwood,* 999 F.2d 86, 92 (4th Cir. 1993).

THE FEDERAL ARBITRATION ACT

As a preliminary matter, Plaintiffs have styled their complaint as one to enforce the arbitrator's award under § 9 of the Federal Arbitration Act, 9 U.S.C. § 1 et seq. (2006), when, in reality, it is a complaint to modify the award under section 10 of that statute. This is so because, although the arbitrator found that only $14,100 of *Chessie*'s hull damage was caused by lightning, Plaintiffs nonetheless ask the Court to award a judgment in the amount of $36,000. Plaintiffs' argument regarding the substance of the agreement between the parties further underscores this conclusion. Specifically, Plaintiffs allege that the parties entered into an "all or nothing" agreement,

whereby the arbitrator was to determine that the hull damage was caused by lightning, and if so, award Plaintiffs the $36,000.00 in damages claimed. Pl.'s MSJ at 5. According to Plaintiffs,

> the Arbitrator's sole function was to determine whether the hull damage, in the agreed-upon amount of $36,000, was caused by the lightning strike occurring on May 17, 2004. The Arbitration Agreement did not grant the Arbitrator the authority to assess a damage amount.

Id. (emphasis added). This argument is consistent with a motion to modify under § 10(b)(4), which permits a federal court to modify or vacate an arbitration award upon a showing that "the arbitrator[] exceeded their powers." Accordingly, the Court will evaluate Plaintiffs' motion under § 10 of the FAA.

In contrast, Markel's complaint truly is one to enforce the arbitrator's award. Markel denies that it entered into an "all or nothing" arbitration agreement with regard to damages, and seeks to enforce the arbitrator's award of $14,100. Def.'s Mot. at 5.

The question before the Court, therefore, is whether the arbitrator exceeded his authority under the arbitration agreement by assigning a value to the damages attributable to the lightning strike that was less than the $36,000 claimed by Plaintiffs. If the answer is yes, then the court can vacate, remand, or modify the award. 9 U.S.C. § 10, 11. If the answer is no, then the court must grant Defendant's motion to confirm the award under § 9 of the FAA.

To resolve whether the arbitrator exceeded his authority, the Court first must determine the scope of the arbitration agreement; specifically, whether the parties agreed to arbitrate the amount of damages caused by the lightning strike. Because the parties did not agree to submit questions of arbitrability to the arbitrator for resolution, determining the scope of the agreement is an issue for the Court to decide. *First Options of Chicago, Inc. v. Kaplan*, 514 U.S. 938, 943 (1995). In this regard, the Supreme Court has advised that, "[w]hen deciding whether the parties agreed to arbitrate

a certain matter . . . courts generally . . . should apply ordinary state-law principles of contract interpretation." *Kaplan*, 514 U.S. at 944, *accord E.I. Dupont De Nemours & Co. v. Martinsville Nylon Employees' Council Corp*., 78 F.3d 578 (4th Cir. 1996). In doing so, the Court must "give due regard to the federal policy favoring arbitration and resolve 'any doubts concerning the scope of arbitrable issues in favor of arbitration." *Hill v. PeopleSoft USA, Inc*., 412 F.3d 540, 543 (4th Cir. 2005) (*quoting Moses H. Cone Mem'l Hosp. v. Mercury Constr. Corp.*, 460 U.S. 1, 24-25 (1983)). Maryland law[2] regarding contract interpretation requires the court first to "determine from the language of the agreement itself what a reasonable person in the position of the parties would have meant at the time it was effectuated." *GMAC v. Daniels*, 303 Md. 254, 262, 492 A.2d 1306, 1310 (Md. 1985). If the language of the contract is clear and unambiguous, then the Court "must presume that the parties meant what they expressed." *Id*. If the language of the contract is ambiguous, however, the court may consider parol evidence to determine the intent of the parties. *E.g. Truck Ins. Exch. v. Marks Rentals, Inc*., 288 Md. 428, 433, 418 A.2d 1187, 1190 (Md. 1980). Contract language is ambiguous if it could be read to have more than one meaning by a reasonably prudent layperson. *Clendenin Bros., Inc. v. United States Fire Ins. Co.*, 390 Md. 449, 459, 889 A.2d 387, 393-394 (Md. 2006), citing *Truck Ins. Exch.*, 288 Md. at 433, 418 A.2d at 1190.

Here, I find that the language of the arbitration agreement is ambiguous; it could be read either to permit the arbitrator to determine the amount of damage to *Chessie*, or to limit his authority to determining only whether the claimed damages were caused by the lightning strike. Under normal circumstances, the Court would look to the documentary evidence provided by the parties, which in this case includes the arbitration agreement, award, and copies of e-mail correspondence between

[2]The parties do not dispute that Maryland law applies.

counsel, ostensibly supplied as extrinsic evidence of the parties' intent with regard to the scope of the arbitration agreement. In this case, however, the admissibility problems with the evidence presented are manifest. First, none of the documentary evidence presented is authenticated by affidavit or otherwise. Next, most of the facts relevant to the contract negotiations at issue have been provided by counsel *ipse dixit*, without supporting affidavits or deposition testimony. The evidentiary problems associated with the copies of e-mail offered as parol evidence likewise are substantial because they were not authenticated, but instead were simply attached to the parties' motions as exhibits.

Because neither party to this dispute complied with the requirements of Rule 56 that they support their motions with admissible evidence, I dismissed both motions without prejudice to allow resubmission with proper evidentiary support. (Paper No. 26). I further observed that the unauthenticated e-mails are a form of computer generated evidence that pose evidentiary issues that are highlighted by their electronic medium. Given the pervasiveness today of electronically prepared and stored records, as opposed to the manually prepared records of the past, counsel must be prepared to recognize and appropriately deal with the evidentiary issues associated with the admissibility of electronically generated and stored evidence. Although cases abound regarding the discoverability of electronic records, research has failed to locate a comprehensive analysis of the many interrelated evidentiary issues associated with electronic evidence. Because there is a need for guidance to the bar regarding this subject, this opinion undertakes a broader and more detailed analysis of these issues than would be required simply to resolve the specific issues presented in this case. It is my hope that it will provide a helpful starting place for understanding the challenges associated with the admissibility of electronic evidence.

ADMISSIBILITY OF ELECTRONICALLY STORED INFORMATION

Be careful what you ask for, the saying goes, because you might actually get it. For the last several years there has been seemingly endless discussion of the rules regarding the discovery of electronically stored information ("ESI"). The adoption of a series of amendments to the Federal Rules of Civil Procedure relating to the discovery of ESI in December of 2006 has only heightened, not lessened, this discussion. Very little has been written, however, about what is required to insure that ESI obtained during discovery is admissible into evidence at trial, or whether it constitutes "such facts as would be admissible in evidence" for use in summary judgment practice. FED. R. CIV. P. 56(e).[3] This is unfortunate, because considering the significant costs associated with discovery of ESI, it makes little sense to go to all the bother and expense to get electronic information only to have it excluded from evidence or rejected from consideration during summary judgment because the proponent cannot lay a sufficient foundation to get it admitted. The process is complicated by the fact that ESI comes in multiple evidentiary "flavors," including e-mail, website ESI, internet postings, digital photographs, and computer-generated documents and data files.[4]

---

[3] *See, e.g. Orsi v. Kirkwood*, 999 F.2d 86, 92 (4th Cir. 1993)("It is well established that unsworn, unauthenticated documents cannot be considered on a motion for summery judgment"); *Planmatics, Inc. v. Showers*, 137 F. Supp.2d 616, 620 (D. Md. 2001) ("On a motion for summary judgment, a district court may only consider evidence that would be admissible at trial" (citations omitted)). *See also Maryland Highway Contractors Assoc., Inc. v. State of Maryland*, 933 F.2d 1246, 1251 (4th Cir. 1991); *Wilson v. Clancy*, 747 F. Supp. 1154,1158 (D. Md. 1990); JACK B. WEINSTEIN & MARGARET A. BERGER, WEINSTEIN'S FEDERAL EVIDENCE § 901.02[1] (Joseph M. McLaughlin ed., Matthew Bender 2d ed. 1997)(hereinafter "WEINSTEIN").

[4]Examples of internet postings include; data posted by the site owner, data posted by others with the consent of the site owner, and data posted by others without consent, such as "hackers." Examples of computer-generated documents and files include; electronically stored records or data, computer simulation, and computer animation. *See* 2 MCCORMICK ON EVIDENCE § 227 (John William Strong, et al. eds., 6th ed. 2006); Gregory P. Joseph, *Internet and Email Evidence*, 13 PRAC. LITIGATOR (Mar. 2002), *reprinted in* 5 STEPHEN A. SALTZBURG ET

Whether ESI is admissible into evidence is determined by a collection of evidence rules [5] that present themselves like a series of hurdles to be cleared by the proponent of the evidence. Failure to clear any of these evidentiary hurdles means that the evidence will not be admissible. Whenever ESI is offered as evidence, either at trial or in summary judgment, the following evidence rules must be considered: (1) is the ESI **relevant** as determined by Rule 401 (does it have any tendency to make some fact that is of consequence to the litigation more or less probable than it otherwise would be); (2) if relevant under 401, is it **authentic** as required by Rule 901(a) (can the proponent show that the ESI is what it purports to be); (3) if the ESI is offered for its substantive truth, is it **hearsay** as defined by Rule 801, and if so, is it covered by an applicable exception (Rules 803, 804 and 807); (4) is the form of the ESI that is being offered as evidence an **original** or **duplicate** under the original writing rule, of if not, is there admissible secondary evidence to prove the content of the ESI (Rules 1001-1008); and (5) is the probative value of the ESI substantially outweighed by the danger of **unfair prejudice** or one of the other factors identified by Rule 403,

---

AL., FEDERAL RULES OF EVIDENCE MANUAL, Part 4 at 20 (9th ed. 2006)(hereinafter "Joseph"); Hon. Paul W. Grimm and Claudia Diamond, *Low-Tech Solutions to High-Tech Wizardry: Computer Generated Evidence*, 37 MD. B. J. 4 (July/August, 2004).

[5] It has been noted that "[t]he Federal Rules of Evidence . . . do not separately address the admissibility of electronic data."ADAM COHEN AND DAVID LENDER, ELECTRONIC DISCOVERY: LAW AND PRACTICE § 6.01 (Aspen Publishers 2007). However, "the Federal Rules of Evidence apply to computerized data as they do to other types of evidence." MANUAL FOR COMPLEX LITIGATION § 11.447 (4th ed. 2004). Indeed, FED. R. EVID. 102 contemplates that the rules of evidence are flexible enough to accommodate future "growth and development" to address technical changes not in existence as of the codification of the rules themselves. Further, courts have had little difficulty using the existing rules of evidence to determine the admissibility of ESI, despite the technical challenges that sometimes must be overcome to do so. *See, e.g., In Re F.P., A Minor,* 878 A.2d 91, 95 (Pa. Super. Ct. 2005) ("Essentially, appellant would have us create a whole new body of law just to deal with e-mails or instant messages . . . . We believe that e-mail messages and similar forms of electronic communications can be properly authenticated within the existing framework of [the state rules of evidence].").

such that it should be excluded despite its relevance. Preliminarily, the process by which the admissibility of ESI is determined is governed by Rule 104, which addresses the relationship between the judge and the jury with regard to preliminary fact finding associated with the admissibility of evidence. Because Rule 104 governs the very process of determining admissibility of ESI, it must be considered first.

Preliminary Rulings on Admissibility(Rule 104)

The relationship between Rule 104(a) and (b) can complicate the process by which ESI is admitted into evidence at trial, or may be considered at summary judgment. The rule states, in relevant part:

> (a) Questions of admissibility generally. Preliminary questions concerning the qualification of a person to be a witness, the existence of a privilege, or the admissibility of evidence shall be determined by the court, subject to the provisions of subdivision (b) . . . . In making its determination it is not bound by the rules of evidence except those with respect to privileges.
>
> (b) Relevancy conditioned on fact. When the relevancy of evidence depends upon the fulfillment of a condition of fact, the court shall admit it upon, or subject to, the introduction of evidence sufficient to support a finding of the fulfillment of the condition.

FED. R. EVID. 104 (a) and (b).

When the judge makes a preliminary determination regarding the admissibility of evidence under Rule 104(a), the Federal Rules of Evidence, except for privilege, do not apply. Rule 104(a), 1101(d)(1). Therefore, the court may consider hearsay or other evidence that would not be admissible if offered to the jury,[6] and "hearings on preliminary matters need not be conducted with

[6] *Precision Piping and Instruments v. E.I. du Pont de Nemours and Co.*, 951 F.2d 613, 621 (4th Cir. 1991); 1 STEPHEN A. SALTZBURG ET AL., FEDERAL RULES OF EVIDENCE MANUAL, 104.03[1][b] (9th ed. 2006)(hereinafter "SALTZBURG"); WEINSTEIN at § 104.11[1][a]; *Id*. at § 901.06[1][c][iii] ("Rule 104(a) provides that inadmissible evidence may be considered in

all the formalities and requirements of a trial."[7] Accordingly, the trial judge may make preliminary determinations in chambers or at a sidebar conference in court.[8]

The following types of preliminary matters typically are determined by the judge under Rule 104(a): whether an expert is qualified, and if so, whether his or her opinions are admissible; existence of a privilege; and whether evidence is hearsay, and if so, if any recognized exception applies.[9]

The interplay between Rule 104(a) and 104(b) can be a bit tricky, which is illustrated by the manner in which evidence, whether ESI or "hard copy," must be authenticated under Rule 901(a). Authentication under Rule 901 is viewed as a subset of relevancy, because "evidence cannot have a tendency to make the existence of a disputed fact more or less likely if the evidence is not that which its proponent claims."[10] Accordingly, "[r]esolution of whether evidence is authentic calls for a factual determination by the jury and admissibility, therefore, is governed by the procedure set forth in Federal Rule of Evidence 104(b) 'relating to matters of conditional relevance generally.'"[11]

---

determining preliminary questions of admissibility under Rule 104(a). However, that provision does not extend to determinations under Rule 104(b), so the court may not consider inadmissible evidence in determinations governed by Rule 104(b). In determining the preliminary question of authenticity under Rule 104(b), therefore, a judge may only consider evidence that is itself admissible.").

[7] WEINSTEIN at § 104.11[3].

[8] *Id.*; *United States v. Branch*, 970 F.2d 1368 (4th Cir. 1992).

[9] WEINSTEIN at §104.02[2].

[10] *Branch*, 970 F.2d at 1370 (citing *United States v. Sliker*, 751 F.2d 477, 497-99 (2d Cir. 1984)).

[11] *Id.*(citation omitted). *See also*, FED. R. EVID. 901(a) advisory committee's notes ("Authentication and identification represent a special aspect of relevancy . . . . This requirement of showing authenticity or identity falls in the category of relevancy dependent upon fulfillment

In essence, determining whether ESI is authentic, and therefore relevant, is a two step process. First, "[b]efore admitting evidence for consideration by the jury, the district court must determine whether its proponent has offered a satisfactory foundation from which the jury could reasonably find that the evidence is authentic."[12] Then, "because authentication is essentially a question of conditional relevancy, the jury ultimately resolves whether evidence admitted for its consideration is that which the proponent claims."[13] As the Fourth Circuit summarized this process:

> Although the district court is charged with making this preliminary determination, because authentication is essentially a question of conditional relevancy, the jury ultimately resolves whether evidence admitted for its consideration is that which the proponent claims. Because the ultimate resolution of authenticity is a question for the jury, in rendering its preliminary decision on whether the proponent of evidence has laid a sufficient foundation for admission the district court must necessarily assess the adequacy of the showing made before the jury.[14]

With respect to this two step process, the Fourth Circuit went on to state:

> [a]n in camera hearing addressing authenticity does not replace the presentation of authenticating evidence before the jury; the district court must revisit this issue at trial. Thus, even though the district court may have ruled during an in camera proceeding that the proponent had presented sufficient evidence to support a finding that [the evidence] was authentic, evidence that would support the same ruling must be presented again, to the jury, before the [evidence] may be admitted.[15]

In short, there is a significant difference between the way that Rule 104(a) and 104(b) operate. Because, under Rule 104(b), the jury, not the court, makes the factual findings that

---

of a condition of fact and is governed by the procedure set forth in Rule 104(b)").

[12] *Branch*, 970 F.2d at 1370 (citing FED. R. EVID. 104(b) advisory committee's note).

[13] *Id.* at 1370-71.

[14] *Id.*(citation omitted)

[15] *Id.*

determine admissibility, the facts introduced must be admissible under the rules of evidence.[16] It is important to understand this relationship when seeking to admit ESI. For example, if an e-mail is offered into evidence, the determination of whether it is authentic would be for the jury to decide under Rule 104(b), and the facts that they consider in making this determination must be admissible into evidence. In contrast, if the ruling on whether the e-mail is an admission by a party opponent or a business record turns on contested facts, the admissibility of those facts will be determined by the judge under 104(a), and the Federal Rules of Evidence, except for privilege, are inapplicable.

Relevance (Rules 401, 402, and 105)

The first evidentiary hurdle to overcome in establishing the admissibility of ESI is to demonstrate that it is relevant, as defined by Federal Rule of Evidence 401, which states:

> "Relevant evidence" means evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence.

Clearly, facts that tend to prove essential elements of the causes of action and affirmative defenses asserted in the pleadings are "of consequence to the litigation," as are facts that tend to undermine or rehabilitate the credibility of the witnesses who will testify. SALTZBURG at § 401.02[8]. So too, however, are background facts that, although they may not prove elements of the claims and defenses, and may not even be disputed, nonetheless routinely are admitted to help the fact finder

[16] *See, e.g., United States v. Safavian*, 435 F. Supp. 2d 36, 41-42 (D.D.C. 2006) (trial judge relied on proffers of government lawyers about facts learned by FBI agents during their investigation to make preliminary determination that e-mails were admissible, but cautioned that at trial the government would have to call witnesses with personal knowledge of facts and not rely on FBI agents' testimony about what others had told them regarding the origin of the e-mails); SALTZBURG at § 901.02[5] ("In order for the trier of fact to make a rational decision as to authenticity [under Rule 104(b)], the foundation evidence must be admissible and it must actually be placed before the jury if the Judge admits the evidence").

understand the issues in the case and the evidence introduced to prove or disprove them. FED. R. EVID. 401 advisory committee's note. It is important to recognize that relevance is not a static concept; evidence is not relevant or irrelevant, occupying some rigid state of all or nothing. SALTZBURG at §401.02[11]. Instead, "[r]elevancy is not an inherent characteristic of any item of evidence but exists only as a relation between an item of evidence and a matter properly provable in the case." FED. R. EVID. 401 advisory committee's note. As recognized by Federal Rule of Evidence 105, evidence may be admissible for one purpose, but not another, or against one party, but not another.[17] Therefore, it is important for the proponent of the evidence to have considered all of the potential purposes for which it is offered, and to be prepared to articulate them to the court if the evidence is challenged. This point is particularly significant, as discussed below, when considering hearsay objections, where disputed evidence may be inadmissible hearsay if offered for its substantive truth, but admissible if offered for a reason other than its literal truth.

In assessing whether evidence is relevant under Rule 401, it also is important to remember that there is a distinction between the admissibility of evidence, and the weight to which it is entitled in the eyes of the fact finder, as Rule 104(e)[18] instructs. To be relevant, evidence does not have to carry any particular weight — it is sufficient if it has "any tendency" to prove or disprove a consequential fact in the litigation. Whether evidence tends to make a consequential fact more

---

[17] FED R. EVID. 105 states: "When evidence which is admissible as to one party or for one purpose but not admissible as to another party or for another purpose is admitted, the court, upon request, shall restrict the evidence to its proper scope and instruct the jury accordingly."

[18] FED. R. EVID. 104(e) states: "[Rule 104] does not limit the right of a party to introduce before the jury evidence relevant to weight or credibility [of evidence that has been admitted by an adverse party]."

probable than it would be without the evidence is not a difficult showing to make. FED. R. EVID. 401 advisory committee's note; SALTZBURG at §401.02[1] ("To be relevant it is enough that the evidence has a *tendency* to make a consequential fact even the least bit more probable or less probable than it would be without the evidence. The question of relevance is thus different from whether evidence is *sufficient* to prove a point.") *See also* WEINSTEIN at § 401.05-06.

The Federal Rules of Evidence are clear: evidence that is not relevant is never admissible. FED. R. EVID. 402. Once evidence has been shown to meet the low threshold of relevance, however, it presumptively is admissible unless the constitution, a statute, rule of evidence or procedure, or case law requires that it be excluded.[19] Thus, the function of all the rules of evidence other than Rule 401 is to help determine whether evidence which in fact is relevant should nonetheless be excluded. FED. R. EVID. 402 advisory committee's note ("Succeeding rules [in Article IV of the rules of evidence] . . . in response to the demands of particular policies, require the exclusion of evidence despite its relevancy."). *See also* SALTZBURG § 402.02[1]-[2].

Establishing that ESI has some relevance generally is not hard for counsel. Articulating all of what may be multiple grounds of relevance is something that is important, though not as frequently done as it should be. Accordingly, evidence that might otherwise be admitted may be excluded because the proponent put all his or her eggs in a single evidentiary basket, which the trial judge views as inapplicable, instead of carefully identifying each potential basis for admissibility. That was not the problem in this case, however, because the e-mail and other documentary evidence

---

[19] *Id.* (stating that "[a]ll relevant evidence is admissible, except as otherwise provided by the Constitution of the United States, by Act of Congress, by these rules, or by other rules prescribed by the Supreme Court pursuant to statutory authority. Evidence which is not relevant is not admissible."); SALTZBURG at § 401.02[1]; WEINSTEIN at § 402.02[1].

attached as exhibits to the summary judgment motions are relevant to determining the scope of the arbitration agreement between the parties, and therefore this evidence meets the requirements of Rule 401. Assuming, as is the case here, the proponent of ESI establishes its relevance and concomitant presumptive admissibility, the next step is to demonstrate that it is authentic. It is this latter step that the parties in this case omitted completely.

Authenticity (Rules 901-902)

In order for ESI to be admissible, it also must be shown to be authentic. Rule 901(a) defines what this entails: "[t]he requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." As already noted, "[a]uthentication and identification represent a special aspect of relevancy . . . . This requirement of showing authenticity or identity falls into the category of relevancy dependent upon fulfillment of a condition of fact and is governed by the procedure set forth in Rule 104(b)." FED. R. EVID. 901 advisory committee's note. The requirement of authentication and identification also insures that evidence is trustworthy, which is especially important in analyzing hearsay issues. Indeed, these two evidentiary concepts often are considered together when determining the admissibility of exhibits or documents.[20] WEINSTEIN at § 901.02[2].

A party seeking to admit an exhibit need only make a prima facie showing that it is what he or she claims it to be. *Id.* at § 901.02[3]. This is not a particularly high barrier to overcome. For

[20] *See, e.g., In Re Vee Vinhnee*, 336 B.R. 437, 444 (B.A.P. 9th 2005) (In considering admissibility of electronically stored business records, the court noted "[o]rdinarily, because the business record foundation commonly covers the ground, the authenticity analysis [under Rule 902(11)] is merged into the business record analysis without formal focus on the question." (citation omitted)).

example, in *United States v. Safavian*, the court analyzed the admissibility of e-mail, noting,

> [t]he question for the court under Rule 901 is whether the proponent of the evidence has 'offered a foundation from which the jury could reasonably find that the evidence is what the proponent says it is . . . .' The Court need not find that the evidence is necessarily what the proponent claims, but only that there is sufficient evidence that the *jury* ultimately might do so.

435 F. Supp. 2d at 38 (citations omitted)). *See also United States v. Meienberg*, 263 F.3d 1177, 1180 (10th Cir. 2001) (analyzing admissibility of printouts of computerized records); *United States v. Tank*, 200 F.3d 627, 630 (9th Cir. 2000) (analyzing admissibility of exhibits reflecting chat room conversations)*; United States v. Reilly*, 33 F.3d 1396, 1404 (3d Cir. 1994)(discussing admissibility of radiotelegrams); *United States v. Howard-Arias*, 679 F.2d 363, 366 (4th Cir. 1982)(addressing chain of authenticity); *Telewizja Polska USA, Inc. v. Echostar Satellite Corp*., 2004 WL 2367740, at *16 (N.D. Ill. Oct. 15, 2004) (analyzing admissibility of the content of a website).

Ironically, however, counsel often fail to meet even this minimal showing when attempting to introduce ESI, which underscores the need to pay careful attention to this requirement. Indeed, the inability to get evidence admitted because of a failure to authenticate it almost always is a self-inflicted injury which can be avoided by thoughtful advance preparation. *See, e.g., In Re Vee Vinhnee*, 336 B.R. 437 (proponent failed properly to authenticate exhibits of electronically stored business records); *United States v. Jackson*, 208 F.3d 633, 638 (7th Cir. 2000) (proponent failed to authenticate exhibits taken from an organization's website); *St. Luke's Cataract and Laser Institute PA v. Sanderson*, 2006 WL 1320242, at *3-4 (M.D. Fla. May 12, 2006) (excluding exhibits because affidavits used to authenticate exhibits showing content of web pages were factually inaccurate and affiants lacked personal knowledge of facts); *Rambus v. Infineon Tech. A.G.*, 348 F. Supp. 2d 698 (E.D. Va. 2004) (proponent failed to authenticate computer generated business records)*; Wady v.*

Provident Life and Accident Ins. Co. of Am., 216 F. Supp. 2d 1060 (C.D. Cal. 2002) (sustaining an objection to affidavit of witness offered to authenticate exhibit that contained documents taken from defendant's website because affiant lacked personal knowledge); *Indianapolis Minority Contractors Assoc. Inc. v. Wiley*, 1998 WL 1988826, at *7 (S.D. Ind. May 13, 1998) (proponent of computer records failed to show that they were from a system capable of producing reliable and accurate results, and therefore, failed to authenticate them).

Although courts have recognized that authentication of ESI may require greater scrutiny than that required for the authentication of "hard copy" documents,[21] they have been quick to reject calls to abandon the existing rules of evidence when doing so. For example, in *In Re F.P. , A Minor* the court addressed the authentication required to introduce transcripts of instant message conversations.

---

[21] In *In Re Vee Vinhnee*, the court addressed the authentication of electronically stored business records. It observed "[a]uthenticating a paperless electronic record, in principle, poses the same issue as for a paper record, the only difference being the format in which the record is maintained . . . . ." However, it quickly noted "[t]he paperless electronic record involves a difference in the format of the record that presents more complicated variations on the authentication problem than for paper records. Ultimately, however, it all boils down to the same question of assurance that the record is what it purports to be." The court did conclude, however, that "it is becoming recognized that early versions of computer foundations were too cursory, even though the basic elements covered the ground," before exercising a demanding analysis of the foundation needed to authenticate a paperless business record and lay the foundation for the business record exception to the hearsay rule, ultimately ruling that a proper foundation had not been established, and excluding the evidence. 336 B.R. at 444-45. *See also* MANUAL FOR COMPLEX LITIGATION at § 11.447 ("In general, the Federal Rules of Evidence apply to computerized data as they do to other types of evidence. Computerized data, however, raise unique issues concerning accuracy and authenticity. Accuracy may be impaired by incomplete data entry, mistakes in output instructions, programming errors, damage and contamination of storage media, power outages, and equipment malfunctions. The integrity of data may also be compromised in the course of discovery by improper search and retrieval techniques, data conversion, or mishandling. The proponent of computerized evidence has the burden of laying a proper foundation by establishing its accuracy. The judge should therefore consider the accuracy and reliability of computerized evidence, including any necessary discovery during pretrial proceedings, so that challenges to the evidence are not made for the first time at trial.").

In rejecting the defendant's challenge to this evidence, it stated:

> Essentially, appellant would have us create a whole new body of law just to deal with e-mails or instant messages. The argument is that e-mails or text messages are inherently unreliable because of their relative anonymity and the fact that while an electronic message can be traced to a particular computer, it can rarely be connected to a specific author with any certainty. Unless the purported author is actually witnessed sending the e-mail, there is always the possibility it is not from whom it claims. As appellant correctly points out, anybody with the right password can gain access to another's e-mail account and send a message ostensibly from that person. However, the same uncertainties exist with traditional written documents. A signature can be forged; a letter can be typed on another's typewriter; distinct letterhead stationary can be copied or stolen. We believe that e-mail messages and similar forms of electronic communication can be properly authenticated within the existing framework of PaR.E. 901 and Pennsylvania case law . . . We see no justification for constructing unique rules of admissibility of electronic communications such as instant messages; they are to be evaluated on a case-by-case basis as any other document to determine whether or not there has been an adequate foundational showing of their relevance and authenticity.

878 A.2d at 95-96. Indeed, courts increasingly are demanding that proponents of evidence obtained from electronically stored information pay more attention to the foundational requirements than has been customary for introducing evidence not produced from electronic sources. As one respected commentator on the Federal Rules of Evidence has noted:

> In general, electronic documents or records that are merely stored in a computer raise no computer-specific authentication issues. If a computer processes data rather than merely storing it, authentication issues may arise. The need for authentication and an explanation of the computer's processing will depend on the complexity and novelty of the computer processing. There are many states in the development of computer data where error can be introduced, which can adversely affect the accuracy and reliability of the output. Inaccurate results occur most often because of bad or incomplete data inputting, but can also happen when defective software programs are used or stored-data media become corrupted or damaged.
>
> The authentication requirements of Rule 901 are designed to set up a threshold preliminary standard to test the reliability of evidence, subject to later review by an opponent's cross-examination. Factors that should be considered in evaluating the reliability of computer-based evidence include the error rate in data inputting, and the security of the systems. The degree of foundation required to authenticate computer-based evidence depends on the quality and completeness of the data input,

> the complexity of the computer processing, the routineness of the computer operation, and the ability to test and verify results of the computer processing.
>
> Determining what degree of foundation is appropriate in any given case is in the judgment of the court. The required foundation will vary not only with the particular circumstances but also with the individual judge.

WEINSTEINat § 900.06[3]. Obviously, there is no "one size fits all" approach that can be taken when authenticating electronic evidence, in part because technology changes so rapidly that it is often new to many judges.

Although Rule 901(a) addresses the requirement to authenticate electronically generated or electronically stored evidence, it is silent regarding how to do so. Rule 901(b), however, provides examples of how authentication may be accomplished. It states:

> (b) Illustrations.
>
> By way of illustration only, and not by way of limitation, the following are examples of authentication or identification conforming with the requirements of this rule:
>
> (1) Testimony of witness with knowledge. Testimony that a matter is what it is claimed to be.
>
> (2) Nonexpert opinion on handwriting. Nonexpert opinion as to the genuineness of handwriting, based upon familiarity not acquired for purposes of the litigation.
>
> (3) Comparison by trier or expert witness. Comparison by the trier of fact or by expert witnesses with specimens which have been authenticated.
>
> (4) Distinctive characteristics and the like. Appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances.
>
> (5) Voice identification. Identification of a voice, whether heard firsthand or through mechanical or electronic transmission or recording, by opinion based upon hearing the voice at any time under circumstances connecting it with the alleged speaker.
>
> (6) Telephone conversations. Telephone conversations, by evidence that a call was made to the number assigned at the time by the telephone company to a particular person or business, if (A) in the case of a person, circumstances, including self-identification, show the person answering to be the one called, or (B) in the case of a business, the call was made to a place of business and the conversation related to business reasonably transacted over the telephone.

> (7) Public records or reports. Evidence that a writing authorized by law to be recorded or filed and in fact recorded or filed in a public office, or a purported public record, report, statement, or data compilation, in any form, is from the public office where items of this nature are kept.
>
> (8) Ancient documents or data compilation. Evidence that a document or data compilation, in any form, (A) is in such condition as to create no suspicion concerning its authenticity, (B) was in a place where it, if authentic, would likely be, and (C) has been in existence 20 years or more at the time it is offered.
>
> (9) Process or system. Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.
>
> (10) Methods provided by statute or rule. Any method of authentication or identification provided by Act of Congress or by other rules prescribed by the Supreme Court pursuant to statutory authority.

The ten methods identified by Rule 901(b) are non-exclusive. FED. R. EVID. 901(b) advisory committee's note ("The examples are not intended as an exclusive enumeration of allowable methods but are meant to guide and suggest, leaving room for growth and development in this area of the law."); WEINSTEIN at §901.03[1] ("Parties may use any of the methods listed in Rule 901(b), any combination of them, or any other proof that may be available to carry their burden of showing that the proffered exhibit is what they claim it to be."); *Telewizja Polska USA*, 2004 WL 2367740 (authentication methods listed in Rule 901(b) are "non-exhaustive"). *See also United States v. Simpson*, 152 F.3d 1241, 1249 (10th Cir. 1998) (evaluating methods of authenticating a printout of the text of a chat room discussion between the defendant and an undercover detective in a child pornography case).

Although the methods of authentication listed in Rule 901(b) "relate for the most part to documents . . . some attention [has been] given to . . . computer print-outs," particularly Rule 901(b)(9), which was drafted with "recent developments" in computer technology in mind. FED. R.

EVID. 901(b) advisory committee's note. When faced with resolving authentication issues for electronic evidence, courts have used a number of the methods discussed in Rule 901(b), as well as approved some methods not included in that rule:

Rule 901(b)(1).

This rule permits authentication by: "[t]estimony that a matter is what it is claimed to be." This rule "contemplates a broad spectrum" including "testimony of a witness who was present at the signing of a document . . . ." FED. R. EVID. 901(a) advisory committee's note. "[I]n recognition of the proponent's light burden of proof in authenticating an exhibit . . . the 'knowledge' requirement of Rule 901(b)(1) is liberally construed. A witness may be appropriately knowledgeable through having participated in or observed the event reflected by the exhibit." WEINSTEIN at § 901.03[2] (cross-reference omitted). Courts considering the admissibility of electronic evidence frequently have acknowledged that it may be authenticated by a witness with personal knowledge. *United States v. Kassimu*, 2006 WL 1880335 (5th Cir. May 12, 2006) (ruling that copies of a post office's computer records could be authenticated by a custodian or other qualified witness with personal knowledge of the procedure that generated the records); *St. Luke's*, 2006 WL 1320242 at *3-4 ("To authenticate printouts from a website, the party proffering the evidence must produce 'some statement or affidavit from someone with knowledge [of the website] . . . for example [a] web master or someone else with personal knowledge would be sufficient.'" (citation omitted)); *Safavian*, 435 F. Supp. 2d at 40 n.2 (D.D.C. 2006) (noting that e-mail may be authenticated by a witness with knowledge that the exhibit is what it is claimed to be); *Wady*, 216 F. Supp 2d 1060 (sustaining objection to affidavit of plaintiff's witness attempting to authenticate documents taken from the defendant's website because the affiant lacked personal knowledge of who maintained the website

or authored the documents). Although Rule 901(b)(1) certainly is met by the testimony of a witness that actually drafted the exhibit, it is not required that the authenticating witness have personal knowledge of the making of a particular exhibit if he or she has personal knowledge of how that type of exhibit is routinely made. WEINSTEIN at § 901.03[2].[22] It is necessary, however, that the authenticating witness provide factual specificity about the process by which the electronically stored information is created, acquired, maintained, and preserved without alteration or change, or the process by which it is produced if the result of a system or process that does so, as opposed to boilerplate, conclusory statements that simply parrot the elements of the business record exception to the hearsay rule, Rule 803(6), or public record exception, Rule 803(8).

Rule 901(b)(3).

This rule allows authentication or identification by "[c]omparison by the trier of fact or by expert witnesses with specimens which have been authenticated." Interestingly, the rule allows either expert opinion testimony to authenticate a questioned document by comparing it to one known to be authentic, or by permitting the factfinder to do so. Obviously, the specimen used for the comparison with the document to be authenticated must be shown itself to be authentic. WEINSTEIN

---

[22] "Oftentimes a witness need not be familiar with specific exhibits to be sufficiently knowledgeable to authenticate or identify them. Business records and records of government agencies, for example, are frequently authenticated by witnesses who have never seen the specific records that comprise the exhibits and know nothing about the specific information they contain. Their authentication is accomplished when a witness identifies the exhibits as documents of a type that the organization typically develops, and testifies about the procedures the organization follows in generating, acquiring, and maintaining documents of that type, and explains the method by which the specific exhibits were retrieved from the organization's files. Similarly, exhibits that are automatically produced upon the occurrence of specified events may be authenticated by the testimony of persons with knowledge of the system or process that results in the production of the exhibit." (footnote omitted)).

at §901.03[7][b]. This may be accomplished by any means allowable by Rule 901 or 902, as well as by using other exhibits already admitted into evidence at trial, or admitted into evidence by judicial notice under Rule 201. *Id.* Although the common law origin of Rule 901(b)(3) involved its use for authenticating handwriting or signatures, FED. R. EVID. 901(b)(3) advisory committee's note, it now is commonly used to authenticate documents, WEINSTEIN at §901.03[7][b], and at least one court has noted its appropriate use for authenticating e-mail. *Safavian*, 435 F. Supp. 2d at 40 (E-mail messages "that are not clearly identifiable on their own can be authenticated . . . by comparison by the trier of fact (the jury) with 'specimens which have been [otherwise] authenticated'—in this case, those e-mails that already have been independently authenticated under Rule 901(b)(4).").

Rule 901(b)(4).

This rule is one of the most frequently used to authenticate e-mail and other electronic records. It permits exhibits to be authenticated or identified by "[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances." The commentary to Rule 901(b)(4) observes '[t]he characteristics of the offered item itself, considered in the light of circumstances, afford authentication techniques in great variety," including authenticating an exhibit by showing that it came from a "particular person by virtue of its disclosing knowledge of facts known peculiarly to him," or authenticating "by content and circumstances indicating it was in reply to a duly authenticated" document. FED. R. EVID. 901(b)(4) advisory committee's note. Use of this rule often is characterized as authentication solely by "circumstantial evidence." WEINSTEIN at §901.03[8]. Courts have recognized this rule as a means to authenticate ESI, including e-mail, text messages and the content of websites. *See United States v. Siddiqui,* 235 F.3d 1318, 1322-23 (11th Cir. 2000) (allowing the authentication of an e-mail entirely by circumstantial evidence, including the presence of the defendant's work e-mail address, content of

which the defendant was familiar with, use of the defendant's nickname, and testimony by witnesses that the defendant spoke to them about the subjects contained in the e-mail); *Safavian*, 435 F. Supp. 2d at 40 (same result regarding e-mail); *In Re F.P., a Minor*, 878 A.2d at 94 (noting that authentication could be accomplished by direct evidence, circumstantial evidence, or both, but ultimately holding that transcripts of instant messaging conversation circumstantially were authenticated based on presence of defendant's screen name, use of defendant's first name, and content of threatening message, which other witnesses had corroborated); *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1153-54 (C.D. Cal. 2002) (admitting website postings as evidence due to circumstantial indicia of authenticity, including dates and presence of identifying web addresses).

One method of authenticating electronic evidence under Rule 901(b)(4) is the use of "hash values" or "hash marks" when making documents. A hash value is :

> A unique numerical identifier that can be assigned to a file, a group of files, or a portion of a file, based on a standard mathematical algorithm applied to the characteristics of the data set. The most commonly used algorithms, known as MD5 and SHA, will generate numerical values so distinctive that the chance that any two data sets will have the same hash value, no matter how similar they appear, is less than one in one billion. 'Hashing' is used to guarantee the authenticity of an original data set and can be used as a digital equivalent of the Bates stamp used in paper document production.[23]

Hash values can be inserted into original electronic documents when they are created to provide them with distinctive characteristics that will permit their authentication under Rule 901(b)(4). Also, they can be used during discovery of electronic records to create a form of electronic "Bates stamp"

---

[23]Federal Judicial Center, *Managing Discovery of Electronic Information: A Pocket Guide for Judges*, Federal Judicial Center, 2007 at 24; *see also Williams v. Sprint/United Mgmt. Comp.*, 230 F.R.D. 640, 655 (D. Kan. 2005).

that will help establish the document as electronic.[24] This underscores a point that counsel often overlook. A party that seeks to introduce its own electronic records may have just as much difficulty authenticating them as one that attempts to introduce the electronic records of an adversary. Because it is so common for multiple versions of electronic documents to exist, it sometimes is difficult to establish that the version that is offered into evidence is the "final" or legally operative version. This can plague a party seeking to introduce a favorable version of its own electronic records, when the adverse party objects that it is not the legally operative version, given the production in discovery of multiple versions. Use of hash values when creating the "final" or "legally operative" version of an electronic record can insert distinctive characteristics into it that allow its authentication under Rule 901(b)(4).

Another way in which electronic evidence may be authenticated under Rule 901(b)(4) is by examining the metadata for the evidence. Metadata,

> commonly described as "data about data," is defined as "information describing the history, tracking, or management of an electronic document." Appendix F to *The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age* defines metadata as "information about a particular data set which describes how, when and by whom it was collected, created, accessed, or modified and how it is formatted (including data demographics such as size, location, storage requirements and media information)." Technical Appendix E to the *Sedona Guidelines* provides an extended description of metadata. It further defines metadata to include "all of the contextual, processing, and use information needed to identify and certify the scope, authenticity, and integrity of active or archival electronic information or records." Some examples of metadata for electronic documents include: a file's name, a file's location (e.g., directory structure or pathname), file format or file type, file size, file dates (e.g., creation date, date of last data modification, date of last data access, and date of last metadata

[24] *See, e.g.*, United States District Court for the District of Maryland, Suggested Protocol for Discovery of Electronically Stored Information 20, http://www.mdd.uscourts.gov/news/news/ESIProtocol.pdf (last visited April 10, 2007) (encouraging parties to discuss use of hash values or "hash marks" when producing electronic records in discovery to facilitate their authentication).

> modification), and file permissions (e.g., who can read the data, who can write to it, who can run it). Some metadata, such as file dates and sizes, can easily be seen by users; other metadata can be hidden or embedded and unavailable to computer users who are not technically adept.

Williams v. Sprint/United Mgmt. Co., 230 F.R.D. at 646 (footnote omitted); Federal Judicial Center, *Managing Discovery of Electronic Information: A Pocket Guide for Judges,* Federal Judicial Center, 2007 at 24-25 (defining metadata as "[i]nformation about a particular data set or document which describes how, when, and by whom the data set or document was collected, created, accessed, or modified . . . "). Recently revised Federal Rule of Civil Procedure 34 permits a party to discover electronically stored information and to identify the form or forms in which it is to be produced. A party therefore can request production of electronically stored information in its "native format", which includes the metadata for the electronic document.[25] Because metadata shows the date, time and identity of the creator of an electronic record, as well as all changes made to it, metadata is a distinctive characteristic of all electronic evidence that can be used to authenticate it under Rule 901(b)(4). Although specific source code markers that constitute metadata can provide a useful method of authenticating electronically stored evidence, this method is not foolproof because,

> [a]n unauthorized person may be able to obtain access to an unattended computer. Moreover, a document or database located on a networked-computer system can be viewed by persons on the network who may modify it. In addition, many network computer systems usually provide for a selected network administrators to override an individual password identification number to gain access when necessary.

---

[25] United States District Court for the District of Maryland, Suggested Protocol for Discovery of Electronically Stored Information 17, http://www.mdd.uscourts.gov/news/news/ESIProtocol.pdf (last visited April 10, 2007) ("When parties have agreed or the Court has ordered the parties to exchange all or some documents as electronic files in Native File format in connection with discovery, the parties should collect and produce said relevant files in Native File formats in a manner that preserves the integrity of the files, including, but not limited to the contents of the file, the Meta-Data (including System Meta-Data, Substantive Meta-Data, and Embedded Meta-Data . . . .").

WEINSTEIN at § 900.01[4][a]; *see also Fennell v. First Step Designs, Ltd.*, 83 F.3d 526, 530 (1st Cir. 1996) (discussing how metadata markers can reflect that a document was modified when in fact it simply was saved to a different location). Despite its lack of conclusiveness, however, metadata certainly is a useful tool for authenticating electronic records by use of distinctive characteristics.

Rule 901(b)(7):

> This Rule permits authentication by:
>
> Public records or reports. Evidence that a writing authorized by law to be recorded or filed and in fact recorded or filed in a public office, or a purported public record, report, statement, or data compilation, in any form, is from the public office where items of this nature are kept.

The commentary to Rule 901(b)(7) recognizes that it applies to computerized public records, noting that "[p]ublic records are regularly authenticated by proof of custody, without more. [Rule 901(b)(7)] extends the principle to include data stored in computers and similar methods, of which increasing use in the public records area may be expected." FED. R. EVID. 901(b)(7) advisory committee's note (citation omitted). To use this rule the "proponent of the evidence need only show that the office from which the records were taken is the legal custodian of the records." WEINSTEIN at § 901.10[2]. This may be done by "[a] certificate of authenticity from the public office; [t]he testimony of an officer who is authorized to attest to custodianship, [or] the testimony of a witness with knowledge that the evidence is in fact from a public office authorized to keep such a record." *Id.* (footnote omitted). Examples of the types of public records that may be authenticated by Rule 901(b)(7) include tax returns, weather bureau records, military records, social security records, INS records, VA records, official records from federal, state and local agencies, judicial records, correctional records, law enforcement records, and data compilations, which may include computer stored records. *Id.*

Courts have recognized the appropriateness of authenticating computer stored public records under Rule 901(b)(7) as well, and observed that under this rule, unlike Rule 901(b)(9), there is no need to show that the computer system producing the public records was reliable or the records accurate. For example, in *United States v. Meienberg*, the court rejected defendant's challenge to the admissibility of a law enforcement agency's computerized records. Defendant argued that the only way they could be authenticated was under Rule 901(b)(9), through proof that they were produced by a system or process capable of producing a reliable result. Defendant further argued that the records had not been shown to be accurate. The appellate court disagreed, holding that the records properly had been authenticated under Rule 901(b)(7), which did not require a showing of accuracy. The court noted that any question regarding the accuracy of the records went to weight rather than admissibility. 263 F.3d at 1181. Thus, a decision to authenticate under Rule 901(b)(7), as opposed to 901(b)(9) may mean that the required foundation is much easier to prove. This underscores the importance of the point previously made, that there may be multiple ways to authenticate a particular computerized record, and careful attention to all the possibilities may reveal a method that significantly eases the burden of authentication.

Rule 901(b)(9):

This Rule recognizes one method of authentication that is particularly useful in authenticating electronic evidence stored in or generated by computers. It authorizes authentication by "[e]vidence describing a process or system used to produce a result and showing that the process or system produces an accurate result." FED. R. EVID. 901(b)(9). This rule was "designed for situations in which the accuracy of a result is dependent upon a process or system which produces

it." FED. R. EVID. 901(b)(9) advisory committee's note. *See also* WEINSTEIN at § 901.12[3];[26] *In Re Vee Vinhnee*, 336 B.R. at 446 ("Rule 901(b)(9), which is designated as an example of a satisfactory authentication, describes the appropriate authentication for results of a process or system and contemplates evidence describing the process or system used to achieve a result and demonstration that the result is accurate. The advisory committee note makes plain that Rule 901(b)(9) was designed to encompass computer-generated evidence. . . ").[27]

Rule 902:

In addition to the non-exclusive methods of authentication identified in Rule 901(b), Rule 902 identifies twelve methods by which documents, including electronic ones, may be authenticated without extrinsic evidence. This is commonly referred to as "self-authentication." The rule states:

---

[26] "Computer output may be authenticated under Rule 901(b)(9) . . . . When the proponent relies on the provisions of Rule 901(b)(9) instead of qualifying the computer-generated information for a hearsay exception, it is common for the proponent to provide evidence of the input procedures and their accuracy, and evidence that the computer was regularly tested for programming errors. At a minimum, the proponent should present evidence sufficient to warrant a finding that the information is trustworthy and provide the opponent with an opportunity to inquire into the accuracy of the computer and of the input procedures."

[27] In *Vinhnee*, the court cited with approval an eleven-step foundational authentication for computer records advocated by one respected academic. *Id.* (citing EDWARD J. IMWINKELRIED, EVIDENTIARY FOUNDATIONS 58-59 (LexisNexis 6th ed. 2005)). Although this foundation is elaborate, and many courts might not be so demanding as to require that it be followed to authenticate computer generated records, the fact that one court already has done so should put prudent counsel on notice that they must pay attention to how they will authenticate computer generated records, and that they should be prepared to do so in a manner that complies with the Federal Rules of Evidence and any governing precedent. The price for failing to do so may be, as in *In re Vee Vinhnee*, exclusion of the exhibit. *See, e.g., Indianapolis Minority Contractors Ass'n. Inc. v. Wiley*, 1998 WL 1988826, at *7 (S.D. Ind. May 13, 1998) ("[A]s a condition precedent to admissibility of computer records, the proponent must establish that the process or system used produces an accurate result, FED. R. EVID. 901(b)(9), and that foundation has not been established. In light of the above, the veracity and reliability of these reports are questionable, and thus [the summary judgment exhibit] will be stricken").

Extrinsic evidence of authenticity as a condition precedent to admissibility is not required with respect to the following:

(1) Domestic public documents under seal. A document bearing a seal purporting to be that of the United States, or of any State, district, Commonwealth, territory, or insular possession thereof, or the Panama Canal Zone, or the Trust Territory of the Pacific Islands, or of a political subdivision, department, officer, or agency thereof, and a signature purporting to be an attestation or execution.

(2) Domestic public documents not under seal. A document purporting to bear the signature in the official capacity of an officer or employee of any entity included in paragraph (1) hereof, having no seal, if a public officer having a seal and having official duties in the district or political subdivision of the officer or employee certifies under seal that the signer has the official capacity and that the signature is genuine.

(3) Foreign public documents. A document purporting to be executed or attested in an official capacity by a person authorized by the laws of a foreign country to make the execution or attestation, and accompanied by a final certification as to the genuineness of the signature and official position (A) of the executing or attesting person, or (B) of any foreign official whose certificate of genuineness of signature and official position relates to the execution or attestation or is in a chain of certificates of genuineness of signature and official position relating to the execution or attestation. A final certification may be made by a secretary of an embassy or legation, consul general, consul, vice consul, or consular agent of the United States, or a diplomatic or consular official of the foreign country assigned or accredited to the United States. If reasonable opportunity has been given to all parties to investigate the authenticity and accuracy of official documents, the court may, for good cause shown, order that they be treated as presumptively authentic without final certification or permit them to be evidenced by an attested summary with or without final certification.

(4) Certified copies of public records. A copy of an official record or report or entry therein, or of a document authorized by law to be recorded or filed and actually recorded or filed in a public office, including data compilations in any form, certified as correct by the custodian or other person authorized to make the certification, by certificate complying with paragraph (1), (2), or (3) of this rule or complying with any Act of Congress or rule prescribed by the Supreme Court pursuant to statutory authority.

(5) Official publications. Books, pamphlets, or other publications purporting to be issued by public authority.

(6) Newspapers and periodicals. Printed materials purporting to be newspapers or periodicals.

(7) Trade inscriptions and the like. Inscriptions, signs, tags, or labels purporting to

have been affixed in the course of business and indicating ownership, control, or origin.

(8) Acknowledged documents. Documents accompanied by a certificate of acknowledgment executed in the manner provided by law by a notary public or other officer authorized by law to take acknowledgments.

(9) Commercial paper and related documents. Commercial paper, signatures thereon, and documents relating thereto to the extent provided by general commercial law.

(10) Presumptions under Acts of Congress. Any signature, document, or other matter declared by Act of Congress to be presumptively or prima facie genuine or authentic.

(11) Certified domestic records of regularly conducted activity. The original or a duplicate of a domestic record of regularly conducted activity that would be admissible under Rule 803(6) if accompanied by a written declaration of its custodian or other qualified person, in a manner complying with any Act of Congress or rule prescribed by the Supreme Court pursuant to statutory authority, certifying that the record:

(A) was made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters;

(B) was kept in the course of the regularly conducted activity; and

(C) was made by the regularly conducted activity as a regular practice.

A party intending to offer a record into evidence under this paragraph must provide written notice of that intention to all adverse parties, and must make the record and declaration available for inspection sufficiently in advance of their offer into evidence to provide an adverse party with a fair opportunity to challenge them.

(12) Certified foreign records of regularly conducted activity. In a civil case, the original or a duplicate of a foreign record of regularly conducted activity that would be admissible under Rule 803(6) if accompanied by a written declaration by its custodian or other qualified person certifying that the record:

(A) was made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters;

(B) was kept in the course of the regularly conducted activity; and

(C) was made by the regularly conducted activity as a regular practice.

The declaration must be signed in a manner that, if falsely made, would subject the maker to criminal penalty under the laws of the country where the declaration is signed. A party intending to offer a record into evidence under this paragraph must provide written notice of that intention to all adverse parties, and must make the

> record and declaration available for inspection sufficiently in advance of their offer into evidence to provide an adverse party with a fair opportunity to challenge them.

The obvious advantage of Rule 902 is that it does not require the sponsoring testimony of any witness to authenticate the exhibit — its admissibility is determined simply by examining the evidence itself, along with any accompanying written declaration or certificate required by Rule 902. The mere fact that the rule permits self-authentication, however, does not foreclose the opposing party from challenging the authenticity. Because Rule 104(b) applies in such cases, the exhibit and the evidence challenging its authenticity goes to the jury, which ultimately determines whether it is authentic. FED. R. EVID. 902 advisory committee's note. Some of the examples contained in Rule 902, such as Rule 902(3) (foreign public documents), 902(4) (certified copies of public records), 902(8) (acknowledged documents), 902(11) (certified copies of domestic records of a regularly conducted activity), and 902(12) (certified foreign records of regularly conducted activity), do require a certificate signed by a custodian or other qualified person to accomplish the self-authentication.

Although all of the examples contained in Rule 902 could be applicable to computerized records, three in particular have been recognized by the courts to authenticate electronic evidence: 902(5) (official publications); 902(7) (trade inscriptions); and, 902(11) (certified domestic records of regularly conducted activity). The first, Rule 902(5), provides:

> (5) Official publications. Books, pamphlets, or other publications purporting to be issued by public authority.

The rule "[dispenses] with preliminary proof of the genuineness of purportedly official publications . . . . [but] does not confer admissibility upon all official publications; it merely provides a means whereby their authenticity may be taken as established for purposes of admissibility." FED. R. EVID.

902(5) advisory committee's note. This means that, to be admissible, the proponent may also need to establish that the official record qualifies as a public record hearsay exception under Rule 803(8). WEINSTEIN at § 902.02[2]. Although the rule is silent regarding the level of government that must authorize the publication, commentators suggest that the list includes the United States, any State, district, commonwealth, territory or insular possession of the United States, the Panama Canal Zone, the Trust Territory of the Pacific islands, or a political subdivision, department, officer, or agency of any of the foregoing. *Id.*

In *Equal Employment Opportunity Commission v. E. I. DuPont De Nemours and Co.*, the court admitted into evidence printouts of postings on the website of the United States Census Bureau as self-authenticating under Rule 902(5). 2004 WL 2347556 (E.D. La. Oct. 18, 2004). Given the frequency with which official publications from government agencies are relevant to litigation and the increasing tendency for such agencies to have their own websites, Rule 902(5) provides a very useful method of authenticating these publications. When combined with the public records exception to the hearsay rule, Rule 803(8), these official publications posted on government agency websites should be admitted into evidence easily.

Rule 902(7) provides that exhibits may be self-authenticated by "[i]nscriptions, signs, tags, or labels purporting to have been affixed in the course of business and indicating ownership, control, or origin." As one commentator has noted, "[u]nder Rule 902(7), labels or tags affixed in the course of business require no authentication. Business e-mails often contain information showing the origin of the transmission and identifying the employer-company. The identification marker alone may be sufficient to authenticate an e-mail under Rule 902(7)." WEINSTEIN at § 900.07[3][c].

Rule 902(11) also is extremely useful because it affords a means of authenticating business records under Rule 803(6), one of the most used hearsay exceptions, without the need for a witness

to testify in person at trial. It provides:

> (11) Certified domestic records of regularly conducted activity. The original or a duplicate of a domestic record of regularly conducted activity that would be admissible under Rule 803(6) if accompanied by a written declaration of its custodian or other qualified person, in a manner complying with any Act of Congress or rule prescribed by the Supreme Court pursuant to statutory authority, certifying that the record:
>
> (A) was made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters;
>
> (B) was kept in the course of the regularly conducted activity; and
>
> (C) was made by the regularly conducted activity as a regular practice.
>
> A party intending to offer a record into evidence under this paragraph must provide written notice of that intention to all adverse parties, and must make the record and declaration available for inspection sufficiently in advance of their offer into evidence to provide an adverse party with a fair opportunity to challenge them.

This rule was added in the 2000 amendments to the Federal Rules of Evidence, and it was intended to "[set] forth a procedure by which parties can authenticate certain records of regularly conducted activity, other than through the testimony of a foundation witness." FED. R. EVID. 902(11) advisory committee's note. Unlike most of the other authentication rules, Rule 902(11) also contains a notice provision, requiring the proponent to provide written notice of the intention to use the rule to all adverse parties and to make available to them the records sufficiently in advance of litigation to permit a fair opportunity to challenge them. WEINSTEIN at § 902.13[2]. Because compliance with Rule 902(11) requires the proponent to establish all the elements of the business record exception to the hearsay rule, Rule 803(6), courts usually analyze the authenticity issue under Rule 902(11) concomitantly with the business record hearsay exception.[28] *Rambus*, 348 F. Supp. 2d at 710 ("Thus, the most appropriate way to view Rule 902(11) is as the functional equivalent of testimony offered

[28]Because the business record exception will be discussed at some length below, the analysis of the requirements of Rule 902(11) will be deferred until that discussion.

to authenticate a business record tendered under Rule 803(6) because the declaration permitted by Rule 902(11) serves the same purpose as authenticating testimony . . . [B]ecause Rule 902[11] contains the same requirements, and almost the same wording, as Rule 803(6), decisions explaining the parallel provisions of Rule 803(6) are helpful in resolving the issues here presented."); *In Re Vee Vinhnee*, 336 B.R. at 444 (stating that in deciding whether to admit business records, the authenticity analysis is merged into the business record analysis).

Finally, as noted at the beginning of this discussion regarding the authenticating electronic records, Rule 901(b) makes clear that the ten examples listed are illustrative only, not exhaustive. In ruling on whether electronic evidence has been properly authenticated, courts have been willing to think "outside of the box" to recognize new ways of authentication. For example, they have held that documents provided to a party during discovery by an opposing party are presumed to be authentic, shifting the burden to the producing party to demonstrate that the evidence that they produced was not authentic. *Indianapolis Minority Contractors Ass'n.*, 1998 WL 1988826, at *6 ("The act of production is an implicit authentication of documents produced . . . . Federal Rule of Evidence 901 provides that '[t]he requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims. Defendants admit that they did produce [the exhibits at issue] . . . . Thus . . . the Defendants cannot have it both ways. They cannot voluntarily produce documents and implicitly represent their authenticity and then contend they cannot be used by the Plaintiffs because the authenticity is lacking." (citation omitted)); *Perfect 10*, 213 F. Supp. 2d at 1153-54 (finding that exhibits of website postings had been properly authenticated for three reasons, including that certain of them had been provided to the plaintiff by the defendant during discovery).

In *Telewizja Polska USA*, the court embraced a non-traditional method of authentication when faced with determining whether exhibits depicting the content of the defendant's website at various dates several years in the past were admissible. 2004 WL 2367740. The plaintiff offered an affidavit from a representative of the Internet Archive Company, which retrieved copies of the defendant's website as it appeared at relevant dates to the litigation though use of its "wayback machine."[29] The defendant objected, contending that the Internet Archive was not a reliable source, and thus the exhibits had not been authenticated. The court disagreed, stating:

> Federal Rule of Evidence 901 'requires only a prima facie showing of genuineness and leaves it to the jury to decide the true authenticity and probative value of the evidence.' Admittedly, the Internet Archive does not fit neatly into any of the non-exhaustive examples listed in Rule 901; the Internet Archive is a relatively new source for archiving websites. Nevertheless, Plaintiff has presented no evidence that the Internet Archive is unreliable or biased. And Plaintiff has neither denied that the exhibit represents the contents of its website on the dates in question, nor come forward with its own evidence challenging the veracity of the exhibit. Under these circumstances, the Court is of the opinion that [the affidavit from the representative of the Internet Archive Company] is sufficient to satisfy Rule 901's threshold requirement for admissibility.

Id. at *6.

Additionally, authentication may be accomplished by the court taking judicial notice under Rule 201 of certain foundational facts needed to authenticate an electronic record. Under this rule, the parties may request the court to take judicial notice of adjudicative facts that are either (1) generally known within the territorial jurisdiction of the trial court, or (2) capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned. FED. R.

[29] The "wayback machine" refers to the process used by the Internet Archive Company, www.archive.org, to allow website visitors to search for archived web pages of organizations. *St. Luke's*, 2006 WL 1320242 at *1.

EVID. 201 (b); WEINSTEIN at § 201.12[1]. Judicial notice could be a helpful way to establish certain well known characteristics of computers, how the internet works, scientific principles underlying calculations performed within computer programs, and many similar facts that could facilitate authenticating electronic evidence.

Authentication also can be accomplished in civil cases by taking advantage of FED. R. CIV. P. 36, which permits a party to request that his or her opponent admit the "genuineness of documents." Also, at a pretrial conference, pursuant to FED. R. CIV. P. 16(c)(3), a party may request that an opposing party agree to stipulate "regarding the authenticity of documents," and the court may take "appropriate action" regarding that request. Similarly, if a party properly makes his or her FED. R. CIV. P. 26(a)(3) pretrial disclosures of documents and exhibits, then the other side has fourteen days in which to file objections. Failure to do so waives all objections other than under Rules 402 or 403, unless the court excuses the waiver for good cause. This means that if the opposing party does not raise authenticity objections within the fourteen days, they are waived.

The above discussion underscores the need for counsel to be creative in identifying methods of authenticating electronic evidence when the facts support a conclusion that the evidence is reliable, accurate, and authentic, regardless of whether there is a particular example in Rules 901 and 902 that neatly fits.

Finally, any serious consideration of the requirement to authenticate electronic evidence needs to acknowledge that, given the wide diversity of such evidence, there is no single approach to authentication that will work in all instances. It is possible, however, to identify certain authentication issues that have been noted by courts and commentators with particular types of electronic evidence and to be forearmed with this knowledge to develop authenticating facts that

address these concerns.

E-mail

There is no form of ESI more ubiquitous than e-mail, and it is the category of ESI at issue in this case. Although courts today have more or less resigned themselves to the fact that "[w]e live in an age of technology and computer use where e-mail communication now is a normal and frequent fact for the majority of this nation's population, and is of particular importance in the professional world," *Safavian*, 435 F. Supp. 2d at 41, it was not very long ago that they took a contrary view —"[e]-mail is far less of a systematic business activity than a monthly inventory printout." *Monotype Corp. PLC v. Int'l Typeface*, 43 F.3d 443, 450 (9th Cir. 2004) (affirming trial court's exclusion of e-mail as inadmissible as a business record). Perhaps because of the spontaneity and informality of e-mail, people tend to reveal more of themselves, for better or worse, than in other more deliberative forms of written communication. For that reason, e-mail evidence often figures prominently in cases where state of mind, motive and intent must be proved. Indeed, it is not unusual to see a case consisting almost entirely of e-mail evidence. *See, e.g.*, *Safavian*, 435 F. Supp. 2d 36.

Not surprisingly, there are many ways in which e-mail evidence may be authenticated. One well respected commentator has observed:

> [E]-mail messages may be authenticated by direct or circumstantial evidence. An e-mail message's distinctive characteristics, including its "contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances" may be sufficient for authentication.
>
> Printouts of e-mail messages ordinarily bear the sender's e-mail address, providing circumstantial evidence that the message was transmitted by the person identified in the e-mail address. In responding to an e-mail message, the person receiving the message may transmit the reply using the computer's reply function, which automatically routes the message to the address from which the original message came. Use of the reply function indicates that the reply message was sent to the

> sender's listed e-mail address.
>
> The contents of the e-mail may help show authentication by revealing details known only to the sender and the person receiving the message.
>
> E-mails may even be self-authenticating. Under Rule 902(7), labels or tags affixed in the course of business require no authentication. Business e-mails often contain information showing the origin of the transmission and identifying the employer-company. The identification marker alone may be sufficient to authenticate an e-mail under Rule 902(7). However, the sending address in an e-mail message is not conclusive, since e-mail messages can be sent by persons other than the named sender. For example, a person with unauthorized access to a computer can transmit e-mail messages under the computer owner's name. Because of the potential for unauthorized transmission of e-mail messages, authentication requires testimony from a person with personal knowledge of the transmission or receipt to ensure its trustworthiness.

WEINSTEIN at § 900.07[3][c]; *see also* EDWARD J. IMWINKELRIED, EVIDENTIARY FOUNDATIONS § 4.03[4][b] (LexisNexis 6th ed. 2005)(hereinafter "IMWINKELRIED, EVIDENTIARY FOUNDATIONS.") Courts also have approved the authentication of e-mail by the above described methods. *See, e.g.*, *Siddiqui*, 235 F.3d at 1322-23 (E-mail may be authenticated entirely by circumstantial evidence, including its distinctive characteristics); *Safavian*, 435 F. Supp. 2d at 40 (recognizing that e-mail may be authenticated by distinctive characteristics (901(b)(4), or by comparison of exemplars with other e-mails that already have been authenticated (901(b)(3)); *Rambus*, 348 F. Supp. 2d 698 (E-mail that qualifies as business record may be self-authenticating under 902(11)); *In Re F.P., A Minor*, 878 A.2d at 94 (E-mail may be authenticated by direct or circumstantial evidence).

The most frequent ways to authenticate e-mail evidence are 901(b)(1) (person with personal knowledge), 901(b)(3) (expert testimony or comparison with authenticated exemplar), 901(b)(4) (distinctive characteristics, including circumstantial evidence), 902(7) (trade inscriptions), and 902(11) (certified copies of business record).

Internet Website Postings

Courts often have been faced with determining the admissibility of exhibits containing representations of the contents of website postings of a party at some point relevant to the litigation. Their reaction has ranged from the famous skepticism expressed in *St.Clair v. Johnny's Oyster and Shrimp, Inc.* 76 F. Supp. 2d 773 (S.D. Tex. 1999),[30] to more permissive approach taken in *Perfect 10*, 213 F. Supp. 2d at 1153-54.[31]

---

[30]There, the court stated that,

> Plaintiff's electronic 'evidence' is totally insufficient to withstand Defendant's Motion to Dismiss. While some look to the Internet as an innovative vehicle for communication, the Court continues to warily and wearily view it largely as one large catalyst for rumor, innuendo, and misinformation. So as to not mince words, the Court reiterates that this so-called Web provides no way of verifying the authenticity of the alleged contentions that Plaintiff wishes to rely upon in his Response to Defendant's Motion. There is no way Plaintiff can overcome the presumption that the information he discovered on the Internet is inherently untrustworthy. Anyone can put anything on the Internet. No web-site is monitored for accuracy and *nothing* contained therein is under oath or even subject to independent verification absent underlying documentation. Moreover, the Court holds no illusions that hackers can adulterate the content on *any* web-site from *any* location at *any* time. For these reasons, any evidence procured off the Internet is adequate for almost nothing, even under the most liberal interpretation of the hearsay exception rules found in FED. R. EVID. 807. Instead of relying on the voodoo information taken from the Internet, Plaintiff must hunt for hard copy back-up documentation in admissible form from the United States Coast Guard or discover alternative information verifying what Plaintiff alleges.

Id. at 774-775.

[31] The court noted that a "reduced evidentiary standard" applied to the authentication of exhibits purporting to depict the defendant's website postings during a preliminary injunction motion. The court found that the exhibits had been authenticated because of circumstantial indicia of authenticity, a failure of the defendant to deny their authenticity, and the fact that the exhibits had been produced in discovery by the defendant. The court declined to require proof that the postings had been done by the defendant or with its authority, or evidence to disprove the possibility that the contents had been altered by third parties.

The issues that have concerned courts include the possibility that third persons other than the sponsor of the website were responsible for the content of the postings, leading many to require proof by the proponent that the organization hosting the website actually posted the statements or authorized their posting. *See United States v. Jackson*, 208 F.3d 633, 638 (7th Cir. 2000) (excluding evidence of website postings because proponent failed to show that sponsoring organization actually posted the statements, as opposed to a third party); *St. Luke's*, 2006 WL 1320242 (plaintiff failed to authenticate exhibits of defendant's website postings because affidavits used to authenticate the exhibits were factually inaccurate and the author lacked personal knowledge of the website); *Wady*, 216 F. Supp. 2d 1060. One commentator has observed "[i]n applying [the authentication standard] to website evidence, there are three questions that must be answered explicitly or implicitly. (1) What was actually on the website? (2) Does the exhibit or testimony accurately reflect it? (3) If so, is it attributable to the owner of the site?"[32] The same author suggests that the following factors will influence courts in ruling whether to admit evidence of internet postings:

> The length of time the data was posted on the site; whether others report having seen it; whether it remains on the website for the court to verify; whether the data is of a type ordinarily posted on that website or websites of similar entities (e.g. financial information from corporations); whether the owner of the site has elsewhere published the same data, in whole or in part; whether others have published the same data, in whole or in part; whether the data has been republished by others who identify the source of the data as the website in question?[33]

Counsel attempting to authenticate exhibits containing information from internet websites need to address these concerns in deciding what method of authentication to use, and the facts to include in the foundation. The authentication rules most likely to apply, singly or in combination, are

---

[32] Joseph at 21; *see also* SALTZBURG at § 901.02[12].

[33] *Id.* at 22.

901(b)(1) (witness with personal knowledge) 901(b)(3) (expert testimony) 901(b)(4) (distinctive characteristics), 901(b)(7) (public records), 901(b)(9) (system or process capable of producing a reliable result), and 902(5) (official publications).

Text Messages and Chat Room Content

Many of the same foundational issues found encountered when authenticating website evidence apply with equal force to text messages and internet chat room content; however, the fact that chat room messages are posted by third parties, often using "screen names" means that it cannot be assumed that the content found in chat rooms was posted with the knowledge or authority of the website host. SALTZBURG at § 901.02[12]. One commentator has suggested that the following foundational requirements must be met to authenticate chat room evidence:

> (1) [e]vidence that the individual used the screen name in question when participating in chat room conversations (either generally or at the site in question); (2) [e]vidence that, when a meeting with the person using the screen name was arranged, the individual . . . showed up; (3) [e]vidence that the person using the screen name identified [himself] as the [person in the chat room conversation]; evidence that the individual had in [his] possession information given to the person using the screen name; (5) [and] [e]vidence from the hard drive of the individual's computer [showing use of the same screen name].

Id. at § 901.02[12]. Courts also have recognized that exhibits of chat room conversations may be authenticated circumstantially. For example, in *In Re F.P. , A Minor,* the defendant argued that the testimony of the internet service provider was required, or that of a forensic expert. 878 A.2d at 93-94. The court held that circumstantial evidence, such as the use of the defendant's screen name in the text message, the use of the defendant's first name, and the subject matter of the messages all could authenticate the transcripts. *Id*. Similarly, in *United States v. Simpson*, the court held that there was ample circumstantial evidence to authenticate printouts of the content of chat room discussions

between the defendant and an undercover detective, including use of the e-mail name of the defendant, the presence of the defendant's correct address in the messages, and notes seized at the defendant's home containing the address, e-mail address and telephone number given by the undercover officer. 152 F.3d at 1249. Likewise, in *United States v. Tank*, the court found sufficient circumstantial facts to authenticate chat room conversations, despite the fact that certain portions of the text of the messages in which the defendant had participated had been deleted. 200 F.3d at 629-31. There, the court found the testimony regarding the limited nature of the deletions by the member of the chat room club who had made the deletions, circumstantial evidence connecting the defendant to the chat room, including the use of the defendant's screen name in the messages, were sufficient to authenticate the messages. *Id.* at 631. Based on the foregoing cases, the rules most likely to be used to authenticate chat room and text messages, alone or in combination, appear to be 901(b)(1) (witness with personal knowledge) and 901(b)(4) (circumstantial evidence of distinctive characteristics).

Computer Stored Records and Data

Given the widespread use of computers, there is an almost limitless variety of records that are stored in or generated by computers. As one commentator has observed "[m]any kinds of computer records and computer-generated information are introduced as real evidence or used as litigation aids at trials. They range from computer printouts of stored digital data to complex computer-generated models performing complicated computations. Each may raise different admissibility issues concerning authentication and other foundational requirements." WEINSTEIN at § 900.06[3]. The least complex admissibility issues are associated with electronically stored records. "In general, electronic documents or records that are merely stored in a computer raise no

computer-specific authentication issues." WEINSTEIN at § 900.06[3]. That said, although computer records are the easiest to authenticate, there is growing recognition that more care is required to authenticate these electronic records than traditional "hard copy" records. MANUAL FOR COMPLEX LITIGATION at § 11.447;[34] *see also* IMWINKELRIED, EVIDENTIARY FOUNDATIONS at 4.03[2].[35]

Two cases illustrate the contrast between the more lenient approach to admissibility of computer records and the more demanding one. In *United States v. Meienberg*, the defendant challenged on appeal the admission into evidence of printouts of computerized records of the Colorado Bureau of Investigation, arguing that they had not been authenticated because the government had failed to introduce any evidence to demonstrate the accuracy of the records. 263 F.3d at1180-81. The Tenth Circuit disagreed, stating:

---

[34]

> Computerized data, however, raise unique issues concerning accuracy and authenticity. Accuracy may be impaired by incomplete data entry, mistakes in output instructions, programming errors, damage and contamination of storage media, power outages, and equipment malfunctions. The integrity of data may also be compromised in the course of discovery by improper search and retrieval techniques, data conversion, or mishandling. The proponent of computerized evidence has the burden of laying a proper foundation by establishing its accuracy.
> The judge should therefore consider the accuracy and reliability of computerized evidence . . . .

[35]

> "In the past, many courts have been lax in applying the authentication requirement to computer records; they have been content with foundational evidence that the business has successfully used the computer system in question and that the witness recognizes the record as output from the computer. However, following the recommendations of the Federal Judicial Center's *Manual for Complex Litigation*, some courts now require more extensive foundation. These courts require the proponent to authenticate a computer record by proving the reliability of the particular computer used, the dependability of the business's input procedures for the computer, the use of proper procedures to obtain the document offered in court, and the witness's recognition of that document as the readout from the computer." (citation omitted).

> Any question as to the accuracy of the printouts, whether resulting from incorrect data entry or the operation of the computer program, as with inaccuracies in any other type of business records, would have affected only the weight of the printouts, not their admissibility.

Id. at 1181 (citation omitted). *See also Kassimu*, 2006 WL 1880335 (To authenticate computer records as business records did not require the maker, or even a custodian of the record, only a witness qualified to explain the record keeping system of the organization to confirm that the requirements of Rule 803(6) had been met, and the inability of a witness to attest to the accuracy of the information entered into the computer did not preclude admissibility); *Sea Land v. Lozen Int'l*, 285 F.3d 808 (9th Cir. 2002) (ruling that trial court properly considered electronically generated bill of lading as an exhibit to a summary judgment motion. The only foundation that was required was that the record was produced from the same electronic information that was generated contemporaneously when the parties entered into their contact. The court did not require evidence that the records were reliable or accurate).

In contrast, in the case of *In Re Vee Vinhnee*, the bankruptcy appellate panel upheld the trial ruling of a bankruptcy judge excluding electronic business records of the credit card issuer of a Chapter 7 debtor, for failing to authenticate them. 336 B.R. 437. The court noted that "it is becoming recognized that early versions of computer foundations were too cursory, even though the basic elements covered the ground." *Id.* at 445-46. The court further observed that:

> The primary authenticity issue in the context of business records is on what has, or may have, happened to the record in the interval between when it was placed in the files and the time of trial. In other words, the record being proffered must be shown to continue to be an accurate representation of the record that originally was created . . . . Hence, the focus is not on the circumstances of the creation of the record, but rather on the circumstances of the preservation of the record during the time it is in the file so as to assure that the document being proffered is the same as the document that originally was created.

Id. at 444. The court reasoned that, for paperless electronic records:

> The logical questions extend beyond the identification of the particular computer equipment and programs used. The entity's policies and procedures for the use of the equipment, database, and programs are important. How access to the pertinent database is controlled and, separately, how access to the specific program is controlled are important questions. How changes in the database are logged or recorded, as well as the structure and implementation of backup systems and audit procedures for assuring the continuing integrity of the database, are pertinent to the question of whether records have been changed since their creation.

Id. at 445. In order to meet the heightened demands for authenticating electronic business records, the court adopted, with some modification, an eleven-step foundation proposed by Professor Edward Imwinkelried:[36]

> Professor Imwinkelried perceives electronic records as a form of scientific evidence and discerns an eleven-step foundation for computer records:
>
> 1. The business uses a computer.
> 2. The computer is reliable.
> 3. The business has developed a procedure for inserting data into the computer.
> 4. The procedure has built-in safeguards to ensure accuracy and identify errors.
> 5. The business keeps the computer in a good state of repair.
> 6. The witness had the computer readout certain data.
> 7. The witness used the proper procedures to obtain the readout.
> 8. The computer was in working order at the time the witness obtained the readout.
> 9. The witness recognizes the exhibit as the readout.
> 10. The witness explains how he or she recognizes the readout.
> 11. If the readout contains strange symbols or terms, the witness explains the meaning of the symbols or terms for the trier of fact.

Id. at 446-47 (citation omitted). Although the position taken by the court in *In Re Vee Vinhnee* appears to be the most demanding requirement for authenticating computer stored records, other courts also have recognized a need to demonstrate the accuracy of these records. *See, e.g., State v.*

---

[36]IMWINKELRIED, EVIDENTIARY FOUNDATIONS at § 4.03[2].

Dunn, 7 S.W.3d 427, 432 (Mo. Ct. App. 2000) (Admissibility of computer-generated records "should be determined on the basis of the reliability and accuracy of the process involved."); *State v. Hall*, 976 S.W.2d 121, 147 (Tenn. 1998) ("[T]he admissibility of the computer tracing system record should be measured by the reliability of the system, itself, relative to its proper functioning and accuracy.").[37]

As the foregoing cases illustrate, there is a wide disparity between the most lenient positions courts have taken in accepting electronic records as authentic and the most demanding requirements that have been imposed. Further, it would not be surprising to find that, to date, more courts have tended towards the lenient rather than the demanding approach. However, it also is plain that commentators and courts increasingly recognize the special characteristics of electronically stored records, and there appears to be a growing awareness, as expressed in the *Manual for Complex Litigation*,[38] that courts "should . . . consider the accuracy and reliability of computerized evidence" in ruling on its admissibility. Lawyers can expect to encounter judges in both camps, and in the absence of controlling precedent in the court where an action is pending setting forth the foundational requirements for computer records, there is uncertainty about which approach will be required. Further, although " it may be better to be lucky than good," as the saying goes, counsel would be wise not to test their luck unnecessarily. If it is critical to the success of your case to admit into evidence computer stored records, it would be prudent to plan to authenticate the record by the most rigorous standard that may be applied. If less is required, then luck was with you.

---

[37] In addition to their insight regarding the authentication of electronic records, these cases are also important in connection to the analysis of whether certain types of electronically stored records constitute hearsay when offered for their substantive truth.

[38] MANUAL FOR COMPLEX LITIGATION at § 11.446.

The methods of authentication most likely to be appropriate for computerized records are 901(b)(1) (witness with personal knowledge), 901(b)(3) (expert testimony), 901(b)(4) (distinctive characteristics), and 901(b)(9) (system or process capable of producing a reliable result).

Computer Animation and Computer Simulations.

Two similar, although distinct, forms of computer generated evidence also raise unique authentication issues. The first is computer animation, "the display of a sequence of computer-generated images." IMWINKELRIED, EVIDENTIARY FOUNDATIONS at § 4.09[4][a]. The attraction of this form of evidence is irresistible, because:

> when there is no movie or video of the event being litigated, a computer animation is a superior method of communicating the relevant information to the trier of fact. Absent a movie or video, the proponent might have to rely on static charts or oral testimony to convey a large amount of complex information to the trier of fact. When the proponent relies solely on oral expert testimony, the details may be presented one at a time; but an animation can piece all the details together for the jury. A computer animation in effect condenses the information into a single evidentiary package. In part due to television, the typical American is a primarily visual learner; and for that reason, in the short term, many jurors find the animation more understandable than charts or oral testimony. Use of an animation can also significantly increase long-term juror retention of the information.

Id. at § 4.09[4][a]. The second form of computer generated evidence is a computer simulation. The distinction between them has been explained usefully as follows:

> Computer generated evidence is an increasingly common form of demonstrative evidence. If the purpose of the computer evidence is to illustrate and explain a witness's testimony, courts usually refer to the evidence as an animation. In contrast, a simulation is based on scientific or physical principles and data entered into a computer, which is programmed to analyze the data and draw a conclusion from it, and courts generally require proof to show the validity of the science before the simulation evidence is admitted
>
> Thus, the classification of a computer-generated exhibit as a simulation or an animation also affects the evidentiary foundation required for its admission.

State v. Sayles, 662 N.W.2d 1, 9 (Iowa 2003) (citation omitted).

Courts generally have allowed the admission of computer animations if authenticated by testimony of a witness with personal knowledge of the content of the animation, upon a showing that it fairly and adequately portrays the facts and that it will help to illustrate the testimony given in the case. This usually is the sponsoring witness. *Id.* at 10 (state's expert witness had knowledge of content of shaken infant syndrome animation and could testify that it correctly and adequately portrayed the facts that would illustrate her testimony); *Hinkle v. City of Clarksburg*, 81 F.3d 416 (4th Cir. 1996) (holding that a computer-animated videotaped recreation of events at issue in trial is not unduly prejudicial if it is sufficiently close to the actual events and is not confused by the jury for the real life events themselves); *Friend v. Time Mfg. Co.*, 2006 WL 2135807, at *7 (D. Ariz. July 28, 2006) ("The use of computer animations is allowed when it satisfies the usual foundational requirements for demonstrative evidence. 'At a minimum, the animation's proponent must show the computer simulation fairly and accurately depicts what it represents, whether through the computer expert who prepared it or some other witness who is qualified to so testify, and the opposing party must be afforded an opportunity for cross-examination.'" (citation omitted)); *People v. Cauley*, 32 P.3d 602 (Colo. 2001) (holding that, "[a] computer animation is admissible as demonstrative evidence if the proponent of the video proves that it: 1) is authentic . . . ; 2) is relevant . . .; 3) is a fair and accurate representation of the evidence to which it relates; and 4) has a probative value that is not substantially outweighed by the danger of unfair prejudice . . ."); *Clark v. Cantrell*, 529 S.E.2d 528 (S.C. 2000) ("[A] party may authenticate a video animation by offering testimony from a witness familiar with the preparation of the animation and the data on which it is based . . . [including] the testimony of the expert who prepared the underlying data and the computer

technician who used that data to create it." (citation omitted)). Thus, the most frequent methods of authenticating computer animations are 901(b)(1) (witness with personal knowledge), and 901(b)(3) (testimony of an expert witness).

Computer simulations are treated as a form of scientific evidence, offered for a substantive, rather than demonstrative purpose. WEINSTEIN at § 900,03[1] (p. 900-21); IMWINKELRIED, EVIDENTIARY FOUNDATIONS at § 4.09[4][a],[c]. The case most often cited with regard to the foundational requirements needed to authenticate a computer simulation is *Commercial Union v. Boston Edison*, where the court stated:

> The function of computer programs like TRACE 'is to perform rapidly and accurately an extensive series of computations not readily accomplished without use of a computer.' We permit experts to base their testimony on calculations performed by hand. There is no reason to prevent them from performing the same calculations, with far greater rapidity and accuracy, on a computer. Therefore . . . we treat computer-generated models or simulations like other scientific tests, and condition admissibility on a sufficient showing that: (1) the computer is functioning properly; (2) the input and underlying equations are sufficiently complete and accurate (and disclosed to the opposing party, so that they may challenge them); and (3) the program is generally accepted by the appropriate community of scientists.

591 N.E.2d 165, 168 (Mass. 1992) (citation omitted). The *Commercial Union* test has been followed by numerous courts in determining the foundation needed to authenticate computer simulations. For example, in *State v. Swinton*, the court cited with approval *Commercial Union*, but added that the key to authenticating computer simulations is to determine their reliability. 847 A.2d 921, 942 (Conn. 2004). In that regard, the court noted that the following problems could arise with this type of computer evidence: (1) the underlying information itself could be unreliable; (2) the entry of the information into the computer could be erroneous; (3) the computer hardware could be unreliable; (4) the computer software programs could be unreliable; (5) "the execution of the instructions, which

transforms the information in some way—for example, by calculating numbers, sorting names, or storing information and retrieving it later" could be unreliable; (6) the output of the computer—the printout, transcript, or graphics, could be flawed; (7) the security system used to control access to the computer could be compromised; and (8) the user of the system could make errors. The court noted that Rule 901(b)(9) was a helpful starting point to address authentication of computer simulations. *Id.; see also Bray v. Bi-State Dev. Corp.*, 949 S.W.2d 93 (Mo. Ct. App. 1997) (citing *Commercial Union* and ruling that authentication properly was accomplished by a witness with knowledge of how the computer program worked, its software, the data used in the calculations, and who verified the accuracy of the calculations made by the computer with manual calculations); *Kudlacek v. Fiat*, 509 N.W.2d 603, (Neb. 1994) (citing *Commercial Union* and holding that computer simulation was authenticated by the plaintiff's expert witness). Thus, the most frequent methods of authenticating computer simulations are 901(b)(1) (witness with personal knowledge); and 901(b)(3) (expert witness). Use of an expert witness to authenticate a computer simulation likely will also involve Federal Rules of Evidence 702 and 703.

Digital Photographs

Photographs have been authenticated for decades under Rule 901(b)(1) by the testimony of a witness familiar with the scene depicted in the photograph who testifies that the photograph fairly and accurately represents the scene. Calling the photographer or offering exert testimony about how a camera works almost never has been required for traditional film photographs. Today, however, the vast majority of photographs taken, and offered as exhibits at trial, are digital photographs, which are not made from film, but rather from images captured by a digital camera and loaded into a computer. Digital photographs present unique authentication problems because they are a form of

electronically produced evidence that may be manipulated and altered. Indeed, unlike photographs made from film, digital photographs may be "enhanced." Digital image "enhancement consists of removing, inserting, or highlighting an aspect of the photograph that the technician wants to change." Edward J. Imwinkelried, *Can this Photo be Trusted?*, Trial, October 2005, at 48. Some examples graphically illustrate the authentication issues associated with digital enhancement of photographs:

> [S]uppose that in a civil case, a shadow on a 35 mm photograph obscures the name of the manufacturer of an offending product. The plaintiff might offer an enhanced image, magically stripping the shadow to reveal the defendant's name. Or suppose that a critical issue is the visibility of a highway hazard. A civil defendant might offer an enhanced image of the stretch of highway to persuade the jury that the plaintiff should have perceived the danger ahead before reaching it. In many criminal trials, the prosecutor offers an 'improved', digitally enhanced image of fingerprints discovered at the crime scene. The digital image reveals incriminating points of similarity that the jury otherwise would never would have seen.

Id. at 49. There are three distinct types of digital photographs that should be considered with respect to authentication analysis: original digital images, digitally converted images, and digitally enhanced images. *Id.*

An original digital photograph may be authenticated the same way as a film photo, by a witness with personal knowledge of the scene depicted who can testify that the photo fairly and accurately depicts it. *Id*. If a question is raised about the reliability of digital photography in general, the court likely could take judicial notice of it under Rule 201. *Id.* For digitally converted images, authentication requires an explanation of the process by which a film photograph was converted to digital format. This would require testimony about the process used to do the conversion, requiring a witness with personal knowledge that the conversion process produces accurate and reliable images, Rules 901(b)(1) and 901(b)(9)-the later rule implicating expert testimony under Rule 702.

Id. Alternatively, if there is a witness familiar with the scene depicted who can testify that the photo produced from the film when it was digitally converted, no testimony would be needed regarding the process of digital conversion. *Id.*

For digitally enhanced images, it is unlikely that there will be a witness who can testify how the original scene looked if, for example, a shadow was removed, or the colors were intensified. In such a case, there will need to be proof, permissible under Rule 901(b)(9), that the digital enhancement process produces reliable and accurate results, which gets into the realm of scientific or technical evidence under Rule 702. *Id.* Recently, one state court has given particular scrutiny to how this should be done. In *State v. Swinton*, the defendant was convicted of murder in part based on evidence of computer enhanced images prepared using the Adobe Photoshop software. 847 A.2d 921, 950-52 (Conn. 2004). The images showed a superimposition of the defendants teeth over digital photographs of bite marks taken from the victim's body. At trial, the state called the forensic odontologist (bite mark expert) to testify that the defendant was the source of the bite marks on the defendant. However, the defendant testified that he was not familiar with how the Adobe Photoshop made the overlay photographs, which involved a multi-step process in which a wax mold of the defendant's teeth was digitally photographed and scanned into the computer to then be superimposed on the photo of the victim. The trial court admitted the exhibits over objection, but the state appellate court reversed, finding that the defendant had not been afforded a chance to challenge the scientific or technical process by which the exhibits had been prepared. The court stated that to authenticate the exhibits would require a sponsoring witness who could testify, adequately and truthfully, as to exactly what the jury was looking at, and the defendant had a right to cross-examine the witness concerning the evidence. Because the witness called by the state to authenticate the exhibits lacked

the computer expertise to do so, the defendant was deprived of the right to cross examine him. *Id.* at 951-51.

Because the process of computer enhancement involves a scientific or technical process, one commentator has suggested the following foundation as a means to authenticate digitally enhanced photographs under Rule 901(b)(9): (1) The witness is an expert in digital photography; (2) the witness testifies as to image enhancement technology, including the creation of the digital image consisting of pixels and the process by which the computer manipulates them; (3) the witness testifies that the processes used are valid; (4) the witness testifies that there has been "adequate research into the specific application of image enhancement technology involved in the case"; (5) the witness testifies that the software used was developed from the research; (6) the witness received a film photograph; (7) the witness digitized the film photograph using the proper procedure, then used the proper procedure to enhance the film photograph in the computer; (8) the witness can identify the trial exhibit as the product of the enchantment process he or she performed. Edward J. Imwinkelried, *Can this Photo be Trusted?*, Trial, October 2005 at 54. The author recognized that this is an "extensive foundation," and whether it will be adopted by courts in the future remains to be seen. *Id*. However, it is probable that courts will require authentication of digitally enhanced photographs by adequate testimony that it is the product of a system or process that produces accurate and reliable results. FED. R. EVID. 901(b)(9).

To prepare properly to address authentication issues associated with electronically generated or stored evidence, a lawyer must identify each category of electronic evidence to be introduced. Then, he or she should determine what courts have required to authenticate this type of evidence, and carefully evaluate the methods of authentication identified in Rules 901 and 902, as well as

consider requesting a stipulation from opposing counsel, or filing a request for admission of the genuineness of the evidence under Rule 36 of the Federal Rules of Civil Procedure. With this analysis in mind, the lawyer then can plan which method or methods of authentication will be most effective, and prepare the necessary formulation, whether through testimony, affidavit, admission or stipulation. The proffering attorney needs to be specific in presenting the authenticating facts and, if authenticity is challenged, should cite authority to support the method selected.

In this case, neither plaintiffs nor defendants provided any authenticating facts for the e-mail and other evidence that they proffered in support of their summary judgment memoranda - they simply attached the exhibits. This complete absence of authentication stripped the exhibits of any evidentiary value because the Court could not consider them as evidentiary facts. This, in turn, required the dismissal, without prejudice, of the cross motions for summary judgment, with leave to resubmit them once the evidentiary deficiencies had been cured.

Hearsay (Rules 801-807)

The fourth "hurdle" that must be overcome when introducing electronic evidence is the potential application of the hearsay rule. Hearsay issues are pervasive when electronically stored and generated evidence is introduced. To properly analyze hearsay issues there are five separate questions that must be answered: (1) does the evidence constitute a **statement**, as defined by Rule 801(a); (2) was the statement made by a "**declarant**," as defined by Rule 801(b); (3) is the statement being offered to prove the **truth of its contents**, as provided by Rule 801(c); (4) is the statement **excluded from the definition of hearsay by rule 801(1)**; and (5) if the statement is hearsay, is it covered by one of the exceptions identified at Rules 803, 804 or 807. It is critical to proper hearsay analysis to consider each of these questions.

The requirements of a "Statement," Rule 801(a), made by a "Person", Rule 801(b)

Rule 801(a) states:

> A "statement" is (1) an oral or written assertion or (2) nonverbal conduct of a person, if it is intended by the person as an assertion."

The key to understanding the hearsay rule is to appreciate that it only applies to intentionally assertive verbal or non-verbal conduct, and its goal is to guard against the risks associated with testimonial evidence: perception, memory, sincerity and narration. FED. R. EVID. 801 advisory committee's note ("The factors to be considered in evaluating the testimony of a witness are perception, memory, and narration. Sometimes a fourth is added, sincerity.")(citations omitted); WEINSTEIN at § 801.11[1] ("To be considered hearsay, a statement out of court must be offered in evidence to prove the truth of the matter it asserts. This part of the definition arises out of the factfinder's need to assess the credibility of the person who made a statement offered for its truth. When a witness testifies in court, the trier can assess the witness's perception, narration and memory to determine whether the testimony accurately represents the facts observed."); PAUL R. RICE, ELECTRONIC EVIDENCE: LAW AND PRACTICE, 262 (ABA Publishing 2005)(hereinafter "RICE") ("Hearsay is an out-of-court statement offered in court to prove the truth of the matter asserted by the out-of-court declarant. It is offered into evidence through the testimony of a witness to that statement or through a written account by the declarant. The hearsay rule excludes such evidence because it possesses the testimonial dangers of perception, memory, sincerity, and ambiguity that cannot be tested through oath and cross-examination.").

The use of the word "statement" in Rule 801(a) is a critical component of the hearsay rule. WEINSTEIN at § 801.10[1] ("Because Rule 801 describes hearsay as an out-of-court *statement*

offered as proof as [sic] the matter asserted, the definition of 'statement' is of critical importance."); SALTZBURG at § 801.02[1][c] ("If proffered evidence is not a 'statement' within the meaning of Rule 801(a), then it cannot be hearsay, and so cannot be excluded under the [hearsay] Rule."). The word is used in a very precise, and non-colloquial sense—it only applies to verbal conduct (spoken or written) or non-verbal conduct that is intended by a human declarant to be *assertive*. The advisory committee note to Rule 801(a) states this concept squarely:

> The definition of 'statement' assumes importance because the term is used in the definition of hearsay in subdivision (c). The effect of the definition of 'statement' is to exclude from the operation of the hearsay rule all evidence of conduct, verbal or nonverbal, not intended as an assertion. The key to the definition is that nothing is an assertion unless intended to be one.

Ironically, the word "assertion" is not defined in the hearsay rule, despite its importance to the concept. An assertion usefully may be defined as "to state as true; declare; maintain." Black's Law Dictionary 106 (5th ed. 1979).

Although there is not universal agreement on this point, it appears that for verbal or nonverbal conduct to fall within the definition of the hearsay rule as defined under the federal rules of evidence, it must be either an expressly assertive written or spoken utterance, or nonverbal conduct expressly intended to be an assertion—the federal rules appear to have excluded from the definition of hearsay "implied assertions"—or unstated assertions that are inferred from verbal or nonverbal conduct. The advisory committee's note to Rule 801(a) supports the notion non-verbal conduct that is not assertive, and verbal conduct (spoken or written)[39] that is non-assertive should

[39] An example of nonassertive written verbal conduct would be to write a person's name and address on an envelope. An example of nonassertive spoken verbal conduct would be to ask a question that does not contain within it a factual assertion "Is it going to rain tomorrow?"

be viewed the same way — falling outside the definition of a "statement:"

> [N]onverbal conduct . . . may be offered as evidence that the person acted as he did because of his belief in the existence of the condition sought to be proved, from which belief the existence of the condition may be inferred. This sequence is, arguably, in effect an assertion of the existence of the condition and hence properly includable within the hearsay concept. Admittedly, evidence of this character is untested with respect to the perception, memory, and narration (or their equivalents) of the actor, but the Advisory Committee is of the view that these dangers are minimal in the absence of an intent to assert and do not justify the loss of the evidence on hearsay grounds. No class of evidence is free of the possibility of fabrication, but the likelihood is less with nonverbal than with assertive verbal conduct. The situations giving rise to the nonverbal conduct are such as virtually to eliminate questions of sincerity . . . . *Similar considerations govern nonasssertive verbal conduct and verbal conduct which is assertive but offered as a basis for inferring something other than the matter asserted, also excluded from the definition of hearsay by the language of subdivision (c).*

FED. R. EVID. 801 (a) advisory committee's note (emphasis added) (citation omitted); *Wilson v. Clancy*, 747 F. Supp. 1154, 1158 (D. Md. 1990) ("It appears to be the intent of the limitation of the hearsay definition under FED. R. EVID. 801(a)(2) to non-verbal conduct 'intended by the [declarant] as an assertion' to do away with the notion that 'implied assertions' are within the hearsay prohibition." (alterations in original) (citation omitted)); WEINSTEIN at § 801.10[2][c] ;[40] SALTZBURG

---

[40] "Words and actions may convey meaning even though they were not consciously intended as assertions. Sometimes the relevance of words or actions to show a particular fact depends on drawing an inference that a person would not have spoken or acted in a certain way unless the person believed a relevant fact to be true. According to the Advisory Committee, the 'key to the definition is that nothing is an assertion unless it is intended to be'. Many courts have found that words or conduct offered to show the actor's implicit beliefs do not constitute statements under the hearsay rule unless they were intended by the actor as an assertion . . . . Other courts, however, have noted that an oral or written declaration is hearsay if offered to show the truth of a matter implied by its contents."

at §801.02[1][c].[41]

The second question that must be answered in the hearsay analysis is closely tied to the first. A writing or spoken utterance cannot be a "statement" under the hearsay rule unless it is made by a "declarant," as required by Rule 801(b), which provides "[a] 'declarant' is a *person* who makes a statement.'" (emphasis added). When an electronically generated record is entirely the product of the functioning of a computerized system or process, such as the "report" generated when a fax is sent showing the number to which the fax was sent and the time it was received, there is no "person" involved in the creation of the record, and no "assertion" being made. For that reason, the record is not a statement and cannot be hearsay.

Cases involving electronic evidence often raise the issue of whether electronic writings constitute "statements" under Rule 801(a). Where the writings are non-assertive, or not made by a "person," courts have held that they do not constitute hearsay, as they are not "statements." *United States v. Khorozian*, 333 F.3d 498, 506 (3d Cir. 2003) ("[N]either the header nor the text of the fax was hearsay. As to the header, '[u]nder FRE 801(a), a statement is something uttered by 'a person,' so nothing 'said' by a machine . . . is hearsay'" (second alteration in original)); *Safavian*, 435 F. Supp. 2d at 44 (holding that portions of e-mail communications that make imperative statements

---

[41] "Common-law jurisdictions divide on whether nonverbal conduct that is not intended as an assertion is hearsay if it is introduced to show the truth of the actor's underlying beliefs . . . . The reasons for excluding non-assertive conduct from the hearsay rule are persuasive. A principal reason for excluding hearsay is that the veracity of the declarant cannot be tested by cross-examination. In the case of non-assertive acts, the actor by definition does not intend to make an assertion, meaning that the risk of insincerity is substantially diminished. The actor is at least not trying to lie. Moreover, non-assertive conduct is usually more reliable than the ordinary out-of-court statement, because by conduct the declarant has risked action on the correctness of his belief—he has put his money where his mouth is."

instructing defendant what to do, or asking questions are nonassertive verbal conduct that does not fit within the definition of hearsay); *Telewizja Polska USA*, 2004 WL 2367740 (finding that images and text posted on website offered to show what the website looked like on a particular day were not "statements" and therefore fell outside the reach of the hearsay rule)*; Perfect 10*, 213 F. Supp. 2d at 1155 (finding that images and text taken from website of defendant not hearsay, "to the extent these images and text are being introduced to show the images and text found on the websites, they are not statements at all—and thus fall outside the ambit of the hearsay rule."); *United States v. Rollins, rev'd on other grounds* 2004 WL 26780, at *9 (A.F. Ct.Crim.App. Dec. 24, 2003)("Computer generated records are not hearsay: the role that the hearsay rule plays in limiting the fact finder's consideration to reliable evidence received from witnesses who are under oath and subject to cross-examination has no application to the computer generated record in this case. Instead, the admissibility of the computer tracing system record should be measured by the reliability of the system itself, relative to its proper functioning and accuracy."); *State v. Dunn*, 7 S.W.3d 427, 432 (Mo. Ct. App. 2000) ("Because records of this type [computer generated telephone records] are not the counterpart of a statement by a human declarant, which should ideally be tested by cross-examination of that declarant, they should not be treated as hearsay, but rather their admissibility should be determined on the reliability and accuracy of the process involved."); *State v. Hall*, 976 S.W.2d 121, 147 (Tenn. 1998) (reviewing the admissibility of computer generated records and holding "[t]he role that the hearsay rule plays in limiting the fact finder's consideration to reliable evidence received from witnesses who are under oath and subject to cross-examination has no application to the computer generated record in this case. Instead, the admissibility of the computer tracing system record should be measured by the reliability of the system, itself, relative to its proper functioning and accuracy.").

The requirement that the statement be offered to prove its substantive truth.

The third question that must be answered in determining if evidence is hearsay is whether the statement is offered to prove its substantive truth, or for some other purpose. Rule 801(c) states: "Hearsay is a statement, other than one made by the declarant while testifying at the trial or hearing, *offered in evidence to prove the truth of the matter asserted*." (emphasis added). Thus, even if the evidence is an assertion, made by a declarant, it still is not hearsay unless offered to prove the truth of what is asserted. The advisory committee's note to Rule 801(c) underscores this: "If the significance of an offered statement lies solely in the fact that it was made, no issue is raised as to the truth of anything asserted, and the statement is not hearsay. The effect is to exclude from hearsay the entire category of 'verbal acts' and 'verbal parts of an act,' in which the statement itself affects the legal rights of the parties or is a circumstance bearing on conduct affecting their rights." FED. R. EVID. 801(c) advisory committee's note (citation omitted). *See also* WEINSTEIN at § 801.11[1] ("'If the significance of an offered statement lies solely in the fact that it was made, no issue is raised as to the truth of anything asserted.' Thus, if a declarant's statement is not offered for its truth, the declarant's credibility is not material, and the statement is not hearsay."(citation omitted)). Commentators have identified many instances in which assertive statements are not hearsay because they are not offered to prove the truth of the assertions: (1) statements offered to prove a claim that the statement was false or misleading, as in a fraud or misrepresentation case;[42] (2) statements offered to "prove that because they were made, listeners had notice or knowledge of the information related in the statements," or to show the effect on the listener of the statement;[43] (3) statements

[42]SALTZBURG at § 801.02[1][e].

[43]*Id*. at § 801.02[1][f]; WEINSTEIN at § 801.11[5][a].

"offered to prove an association between two or more persons;"[44] (4) statements offered as circumstantial evidence of the declarant's state of mind,[45] or motive;[46] (5) statements that have relevance simply because they were made, regardless of their literal truth or falsity—the so called "verbal acts or parts of acts,"[47] also referred to as "legally operative facts";[48] and (6) statements that are questions or imperative commands,[49] such as "what time is it" or "close the door."

When analyzing the admissibility of electronically generated evidence, courts also have held that statements contained within such evidence fall outside the hearsay definition if offered for a purpose other than their substantive truth. *Siddiqui*, 235 F.3d at 1323 (e-mail between defendant and co-worker not hearsay because not offered to prove truth of substantive content, but instead to show that a relationship existed between defendant and co-worker, and that it was customary for them to communicate by e-mail); *Safavian*, 435 F. Supp. 2d at 44 (e-mail from lobbyist to defendant not hearsay because they were not offered to prove their truth, but to illustrate the nature of the lobbyist's work on behalf of clients to provide context for other admissible e-mail; and as evidence of the defendant's intent, motive and state of mind); *Telewizja Polska USA*, 2004 WL 2367740;

---

[44] SALTZBURG at § 801.2[1][g]; *see also* WEINSTEIN at § 801.11[6].

[45] SALTZBURG at § 801.02[1][h]. This category typically deals with statements from which the declarant's state of mind is circumstantially inferred. For example, if someone says "Woe is me" it may be inferred that they are depressed or sad. Such statements are in contrast to statements that constitute direct evidence of the declarant's state of mind, offered to prove that state of mind, for example "I feel good," offered to prove that the declarant felt good. The later example is hearsay, but covered by an exception, Rule 803(3): Then existing state of mind or condition.

[46] WEINSTEIN at § 801.11[5][a],[c].

[47] SALTZBURG at §801.02[1][j].

[48] WEINSTEIN at § 801.11[3]-[4].

[49] *Id.* at § 801.11[2].

Perfect 10, 213 F. Supp at 1155 (exhibits of defendant's website on a particular date were not "statements" for purposes of hearsay rule because they were offered to show trademark and copyright infringement, therefore they were relevant for a purpose other than their literal truth); *State v. Braidic*, 2004 WL 52412 at *1 (Wash. App. Jan. 13, 2004) (e-mail sent by defendant to victim not hearsay because they were not offered to prove the truth of the statements.).

Finally, of particular relevance to this suit are the cases that have held that communications between the parties to a contract that define the terms of a contract, or prove its content, are not hearsay, as they are verbal acts or legally operative facts. *See, e.g.*, *Preferred Properties Inc. v. Indian River Estates Inc*., 276 F.3d 790, 799 n. 5 (6th Cir. 2002) (verbal acts creating a contract are not hearsay); *Kepner-Tegue Inc. v. Leadership Software*, 12 F.3d 527, 540 (5th Cir. 1994) (finding contract to be a signed writing of independent legal significance and therefore non-hearsay); *Mueller v. Abdnor*, 972 F.2d 931, 937 (8th Cir. 1992) (holding contracts and letters from attorney relating to the formation thereof are non-hearsay); *United States v. Tann*, 425 F. Supp. 2d 26, 29 (D.D.C. 2006) (finding negotiable instruments to be legally operative documents that do not constitute hearsay); *Planmatics*, 137 F. Supp. 2d at 621 (D. Md. 2001) (holding testimony regarding instructions made to individuals is not hearsay because instructions were not statements of fact). *See also* WEINSTEIN at § 801.11[3].[50] Because the e-mails that the parties to this suit attached as unauthenticated exhibits to their summary judgment papers were introduced for the purpose of

---

[50] A verbal act is an utterance of an operative fact that gives rise to legal consequences. Verbal acts, also known as statements of legal consequence, are not hearsay, because the statement is admitted merely to show that it was actually made, not to prove the truth of what was asserted in it. For example, the hearsay rule does not exclude relevant evidence as to what the contracting parties said or wrote with respect to the making or the terms of an agreement.

proving the making of the agreement to arbitrate the dispute regarding the damage caused by the lightning strike, and the terms of this agreement, they are not hearsay if offered for this purpose because they are verbal acts, or legally operative facts. What the parties did not do, however, was articulate the non-hearsay purpose for which the e-mails were offered; they merely attached them as exhibits, without further explanation of the purpose for which they were offered, or clarification that they were not offered for their substantive truth. Because evidence may be offered for more than one purpose, it may be relevant for its substantive truth, and potentially hearsay, or relevant for some other purpose, and non-hearsay. For this reason it is important for a party offering an exhibit into evidence to clearly explain each purpose for which it is offered, and address any hearsay issues associated with each purpose for which it is offered.

Is the evidence excluded from the definition of hearsay by Rule 801(d)(1) or 801(d)(2).

Once it has been determined whether evidence falls into the definition of hearsay because it is a statement, uttered by a declarant, and offered for its substantive truth, the final step in assessing whether it is hearsay is to see if it is excluded from the definition of hearsay by two rules: 801(d)(1), which identifies three types of prior statements by witnesses who actually testify and are subject to cross examination, which are excluded from the definition of hearsay, and 801(d)(2), which identifies five types of admissions by a party opponent that are excluded from the definition of hearsay. FED. R. EVID. 801(d) advisory committee's note ("[s]everal types of statements which would otherwise literally fall within the definition [of hearsay] are expressly excluded from it ... "); WEINSTEIN at § 801[20][1] & [801[30][1]; SALTZBURG at § 801.02[2] & 801.02[6].

Rule 801(d)(1) identifies three types of prior witness statements that are excluded from the definition of hearsay: first, 801(d)(1)(A) excludes prior inconsistent "testimonial statements" made under oath at a trial, hearing, court proceeding or deposition; next, 801(d)(1)(B) excludes prior

consistent statements offered to rebut an express or implied allegation of recent fabrication, or improper influence or motive; and finally, 801(d)(1)(C) excludes statements of identification of a person made after perceiving that person. For each of these exceptions, it is required that the declarant testify at trial and be subject to cross examination about the prior statements. FED. R. EVID 801(d)(1); FED. R. EVID. 801(d)(1) advisory committee's note ("[Rule 801(d)(1)] requires in each instance, as a general safeguard, that the declarant actually testify as a witness, and it then enumerates three situations in which the statement is excepted from the category of hearsay."); WEINSTEIN at § 801.20[2] ("For a prior witness statement to escape the hearsay rule, the declarant must testify at trial and be subject to cross-examination concerning the statement." (citation omitted)).

Rule 801(d)(2) identifies five types of statements as "admissions by a party opponent," and excludes them from the definition of hearsay. Specifically: 801(d)(2)(A) excludes the party's own statement, made in either an individual or representative capacity; 801(d)(2)(B) addresses a statement by another that a party has adopted or manifested a belief in its truth; 801(d)(2)(C) deals with a statement by a person authorized by a party to make a statement concerning a subject; 801(d)(2)(D) excludes a statement made by a party's agent or servant concerning a matter within the scope of the agency or employment, made during the existence of the agency or employment relationship; and 801(d)(2)(E) excludes the statement of a co-conspirator of a party made during the existence of the conspiracy and in furtherance of the conspiracy. To qualify as an admission, the party's out-of-court statement must be offered against that party, it cannot offer its own out of court statements as admissions. WEINSTEIN at § 801.30[1] ("To be admissible under [Rule 801(d)(2)], the party's statements must be offered *against* that party. A party cannot use this provision to offer his or her own statements into evidence.").

As can be seen from reading Rule 801(d)(1) and (2), there are specific foundational facts that must be established before the statement or admission can be accepted into evidence. These determinations are made by the trial judge under Rule 104(a), and therefore the rules of evidence, except for privilege, are inapplicable. FED. R. EVID. 104(a),1101(d)(1); FED. R. EVID.104(a) advisory committee's note ("[W]hen a hearsay statement is offered as a declaration against interest, a decision must be made whether it possesses the required against-interest characteristics. These decisions too, are made by the judge.")

Given the near universal use of electronic means of communication, it is not surprising that statements contained in electronically made or stored evidence often have been found to qualify as admissions by a party opponent if offered against that party. *Siddiqui*, 235 F.3d at 1323 (ruling that e-mail authored by defendant was not hearsay because it was an admission under Rule 801(d)(2)(A)); *Safavian*, 435 F. Supp. 2d at 43-44 (holding that e-mail sent by defendant himself was admissible as non-hearsay because it constituted an admission by the defendant, 801(d)(2)(A), and as an "adoptive admission" under Rule 801(d)(2)(B)); *Telewizja Polska USA*, 2004 WL 2367740 (N.D. Ill. Oct. 15, 2004) (holding exhibits showing defendant's website as it appeared on a certain day were admissible as admissions against defendant); *Perfect 10,* 213 F. Supp. 2d at 1155 (admitting e-mail sent by employees of defendant against the defendant as admissions under 801(d)(2)(D)).

If, after applying the foregoing four-step analysis, it is determined that the electronic evidence constitutes a statement by a person that is offered for its substantive truth and is not excluded from the definition of hearsay by Rule 801(d)(1) or (2), then the evidence is hearsay, and is inadmissible unless it qualifies as one of many hearsay exceptions identified by Rule 803, 804 and 807. The process of determining whether hearsay falls into one of the many exceptions can appear daunting,

because there are twenty-three identified in Rule 803, five in Rule 804, and Rule 807, the so-called "catch-all" exception, allows exceptions to be tailor made. Upon closer examination, however, the task is less onerous because the number of hearsay exceptions can be categorized in helpful ways that make them more manageable, and in most instances a handful of hearsay exceptions repeatedly are used in connection with electronically generated or stored evidence. Familiarity with these rules will suffice in most instances to overcome hearsay objections routinely made to ESI.

Rule 803 contains twenty-three separate hearsay exceptions. At first glance they may seem like they have nothing in common, but they do. All twenty-three are admissible regardless of whether the declarant is available to testify, distinguishing them from the five exceptions in Rule 804, each of which is inapplicable unless the declarant is "unavailable," as defined by any of the five methods identified in Rule 804(a). In addition, the twenty-three exceptions in Rule 803 may be grouped in three broad categories: **Category 1** includes exceptions dealing with **perceptions, observations, state of mind, intent and sensation** (803(1) (present sense impressions); 803(2) (excited utterances); 803(3) (then existing state of mind, condition or sensation); 803(4) (statements in furtherance of medical diagnosis and treatment). **Category 2** includes **documents, records, and other writings** (803(5) (past recollection recorded); 803(6) & (7) (business records); 803(8) & (10) (public records); 803(9) (records of vital statistics); 803(11) (records of religious organizations); 803(12 (certificates of baptism, marriage and related events); 803(13) (family records); 803(14) (records of documents affecting an interest in property); 803(15) (statements in documents affecting an interest in property); 803(16) (ancient documents); 803(18 (learned treatises); 803(22) (judgments of conviction in a criminal case); and 803(23) (judgments in certain kinds of civil cases). **Category 3** includes statements dealing with **reputation** (803(19) (reputation regarding personal or family

history); 803(20) (reputation regarding custom, use and practice associated with land, and historically significant facts); and 803(21) (reputation regarding character within the community and among associates).

Given the widely accepted fact that most writings today are created and stored in electronic format, it is easy to see that the many types of documents and writings covered in Rule 803 will implicate electronic writings. Similarly, given the ubiquity of communications in electronic media (e-mail, text messages, chat rooms, internet postings on servers like "myspace" or "youtube" or on blogs, voice mail, etc.), it is not surprising that many statements involving observations of events surrounding us, statements regarding how we feel, our plans and motives, and our feelings (emotional and physical) will be communicated in electronic medium. It would unnecessarily prolong an already lengthy opinion to analyze all of the implications of the hearsay exceptions in Rule 803 as they relate to ESI. It is possible, however, to focus on the handful that have been discussed by the courts and that are most likely to be used in a hearsay analysis of ESI. Because the court's research has shown that the Rule 803 hearsay exceptions, rather than those found in Rules 804 or 807, have been cited by courts evaluating the hearsay implications of electronic evidence, the following analysis will be confined to that rule.

Rule 803(1) Present Sense Impression

Rule 803(1) creates an exception from exclusion under the hearsay rule for:

> (1) Present sense impression. A statement describing or explaining an event or condition made while the declarant was perceiving the event or condition, or immediately thereafter.

There are three elements that must be met for this hearsay exception to apply: (1) the declarant must have personally perceived the event that is described in the statement; (2) the statement must be a simple explanation or description of the event perceived; and (3) the declaration and the event

described must be contemporaneous. WEINSTEIN at § 803.03[1]. Present sense impressions are considered trustworthy because the near simultaneous expression of the explanation or description of the event with its perception militates against any memory deficiency, or opportunity to intentionally misstate what occurred. FED. R. EVID. 803(1) advisory committee's note ("The underlying theory of Exception (1) is that substantial contemporaneity of event and statement negate the likelihood of deliberate or conscious misrepresentation."); WEINSTEIN at § 803.03[1].

Rule 803(2) Excited Utterance

Closely related to Rule 803(1) is Rule 803(2),[51] the excited utterance exception to the hearsay rule, which provides:

> (2) Excited utterance. A statement relating to a startling event or condition made while the declarant was under the stress of excitement caused by the event or condition.

The theory behind the excited utterance exception is that perception of a startling or exciting event produces in the declarant an emotional state that reduces the likelihood that the description of the event while under this emotional state will be inaccurate or purposely misstated. FED. R. EVID. 803(2) advisory committee's note ("The theory of Exception (2) is simply that circumstances may produce a condition of excitement which temporarily stills the capacity of reflection and produces utterances free of conscious fabrication."); WEINSTEIN at § 803.04[1] ("The premise underlying the exception for excited utterances is that a person under the influence of excitement precipitated by an external startling event will not have the reflective capacity essential for fabrication.").

The prevalence of electronic communication devices, and the fact that many are portable and

---

[51] *See* FED. R. EVID. 803(1)-(2) advisory committee's note ("Exceptions (1) and (2) [to Rule 803]. In considerable measure these two examples overlap, though based on somewhat different theories. The most significant practical difference will lie in the time lapse allowable between the event and statement.").

small, means that people always seem to have their laptops, PDA's, and cell phones with them, and available for use to send e-mails or text messages describing events as the are happening. Further, it is a common experience these days to talk to someone on the phone and hear them typing notes of the conversation on a computer as you are talking to them. For these reasons, Rules 803(1) and (2) may provide hearsay exceptions for electronically stored communications containing either present sense impressions or excited utterances. *See, e.g., United States v. Ferber*, 966 F. Supp. 90 (D. Mass. 1997) (holding that e-mail from employee to boss about substance of telephone call with defendant in mail/wire fraud case did qualify as a present sense expression under Rule 803(1), but did not qualify as an excited utterance under Rule 803(2), despite the language at the end of the e-mail "my mind is mush."); *State of New York v. Microsoft*, 2002 WL 649951 (D.D.C. Apr. 12, 2002) (analyzing the admissibility of series of exhibits including e-mail and e-mail "chains" under various hearsay exceptions, and ruling that an e-mail prepared several days after a telephone call that described the call did not qualify as a present sense impression under Rule 803(1) because the requirement of "contemporaneity" was not met).

Rule 803(3) Then Existing State of Mind or Condition

> Rule 803(3) provides a hearsay exception for:
>
> > (3) Then existing mental, emotional, or physical condition. A statement of the declarant's then existing state of mind, emotion, sensation, or physical condition (such as intent, plan, motive, design, mental feeling, pain, and bodily health), but not including a statement of memory or belief to prove the fact remembered or believed unless it relates to the execution, revocation, identification, or terms of declarant's will.

Rule 803(3) also is closely related to Rule 803(1). *See* FED. R. EVID. 803(3) advisory committee's note ("Exception (3) [to Rule 803] is essentially a specialized application of Exception (1), presented separately to enhance its usefulness and accessibility."). The rule permits the statement of the

declarant's state of mind, sensation, mental, emotional, or physical condition, as well as statements of motive, intent, plan or design, but excludes statements of memory or belief if offered to prove the truth of the fact remembered. FED. R. EVID. 803(3) advisory committee's note ("The exclusion of 'statements of memory or belief to prove the fact remembered or believed' is necessary to avoid the virtual destruction of the hearsay rule which would otherwise result from allowing state of mind, provable by a hearsay statement, to serve as the basis for an inference of the happening of the event which produced the state of mind."). The foundation for proving an exception under Rule 803(3) is: (1) The statement must be contemporaneous with the mental state being proven; (2) There must be [an absence of] suspicious circumstances that would evidence a motive for fabrication or misrepresentation of the declarant's state of mind; and (3) The state of mind of the declarant must be relevant in the case. WEINSTEIN at § 803.05[2][a]. Rule 803(3) has been used to prove a wide variety of matters, including the reason why the declarant would not deal with a supplier or dealer, motive, competency, ill-will, motive, lack of intent to defraud, willingness to engage in criminal conduct, the victim's state of mind in an extortion case, and confusion or secondary meaning in a trademark infringement case. *Id.*

Rule 803(3) is particularly useful when trying to admit e-mail, a medium of communication that seems particularly prone to candid, perhaps too-candid, statements of the declarant's state of mind, feelings, emotions, and motives. Indeed, courts have analyzed this rule in connection with ruling on the admissibility of electronic evidence. In *New York v. Microsoft*, the court analyzed admissibility of e-mail and e-mail chains under a variety of hearsay rules, including 803(3). 2002 WL 649951. It concluded that an e-mail made several days following a telephone conversation did not qualify under Rule 803(3) because it contained more than just the declarant's state of mind, but also included the maker's memory of belief about the events that affected his state of mind, which is

specifically excluded by Rule 803(3)). *Id.* at *5. *See also Safavian*, 435 F. Supp. 2d at 44 (admitting e-mail that contained statements of defendant's state of mind under Rule 803(3)).

Rule 803(6) Business Records

Rule 803(6) recognizes an exception to the hearsay rule for:

> (6) Records of regularly conducted activity. A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record or data compilation, all as shown by the testimony of the custodian or other qualified witness, or by certification that complies with Rule 902(11), Rule 902(12), or a statute permitting certification, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness. The term "business" as used in this paragraph includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit.

The foundational elements for a business record are: (1) The document must have been prepared in the normal course of business; (2) it must have been made at or near the time of the events it records; (3) it must be based on the personal knowledge of the entrant or of an informant who had a business duty to transmit the information to the entrant;[52] and (4) to have been made in the normal course of

[52] The majority view is that the source of the information memorialized in the business record must have a business duty to transmit the information to the maker of the record, if the maker him or herself lacks personal knowledge of the facts or events. *See, e.g.,* FED. R. EVID. 803(3) advisory committee's note ("Sources of information presented no substantial problem with ordinary business records. All participants, including the observer or participant furnishing the information to be recorded, were acting routinely, under a duty of accuracy, with the employer reliance on the result, or in short 'in the regular course of business'. If, however, the supplier of the information does not act in the regular course, an essential link is broken; the assurance of accuracy does not extend to the information itself, and the fact that it may be recorded with scrupulous accuracy is of no avail."). However, some courts have held that it may be possible to meet the requirements of the business record exception even if the source of the information had no business duty to provide it to the maker of the record, provided the recipient of the information has a business duty to verify the accuracy of the information provided. *See, e.g., Rambus,* 348 F. Supp. 2d at 706-07 (Court noted that ordinarily, when the supplier of the information recorded in the business record does not act in the regular course of the business, an "essential link" in the foundation is broken, but recognized that "[w]hen the source of the

business means that the document was made in the regular course of a regularly conducted business activity, for which it was the regular practice of the business to maintain a memorandum. WEINSTEIN at § 803.08[1]. It is essential for the exception to apply that it was made in furtherance of the business' needs, and not for the personal purposes of the person who made it. Given the fact that many employees use the computers where they work for personal as well as business reasons, some care must be taken to analyze whether the business record exception is applicable, especially to e-mail.

Rule 902(11) also is helpful in establishing the foundation elements for a business record without the need to call a sponsoring witness to authenticate the document and establish the elements of the hearsay exception. Rule 902(11) permits the self-authentication of a business record by showing the following:

> (11) Certified domestic records of regularly conducted activity. The original or a duplicate of a domestic record of regularly conducted activity that would be admissible under Rule 803(6) if accompanied by a written declaration of its custodian or other qualified person, in a manner complying with any Act of Congress or rule prescribed by the Supreme Court pursuant to statutory authority, certifying that the record–
>
> > (A) was made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters;
> > (B) was kept in the course of the regularly conducted activity; and
> > (C) was made by the regularly conducted activity as a regular practice.
>
> A party intending to offer a record into evidence under this paragraph must provide written notice of that intention to all adverse parties, and must make the record and declaration available for inspection sufficiently in advance of their offer into evidence to provide an adverse party with a fair opportunity to challenge them.

---

information in the business record is an outsider, the only way to save the record from the jaws of the hearsay exclusion is to establish that the business recipient took precautions to guarantee the accuracy of the given information. Thus, the company must have been able in some way to verify the information provided."(citation omitted)).

Because the elements for both rules are essentially identical, they frequently are analyzed together when Rule 902(11) is the proffered means by which a party seek to admit a business record. *See In Re Vee Vinhnee*, 336 B.R. at 446; *Rambus*, 348 F. Supp. 2d at 701 (holding that analysis of Rule 803(6) and 902(11) go "hand in hand," and identifying the following requirements for authentication under Rule 902(11): (1) a qualified custodian or other person having personal knowledge makes the authenticating declaration, who must have "sufficient knowledge of the record-keeping system and the creation of the contested record to establish their trustworthiness;" (2) the declaration must establish that the record was made at or near the time of the occurrence or matters set forth in the document by someone with personal knowledge of these matters or from information provided by someone with personal knowledge thereof; (3) the declaration must show that the record is kept in the course of the regularly conducted activity of the business, and the "mere presence of a document . . . in the retained file of a business entity do[es] not by itself qualify as a record of a regularly conducted activity"; and (4) the declaration must establish that it is the regular practice of the business to keep records of a regularly conducted activity of the business, and "it is not enough if it is the regular practice of an employee to maintain the record of the regularly conducted activity . . . . it must be the regular practice of the business entity to do so"— i.e. it is at the direction of the company that the employee maintain the record).

The business record exception is one of the hearsay exceptions most discussed by courts when ruling on the admissibility of electronic evidence. The decisions demonstrate a continuum running from cases where the court was very lenient in admitting electronic business records, without demanding analysis, to those in which the court took a very demanding approach and scrupulously analyzed every element of the exception, and excluded evidence when all were not

met. For example, in *State of New York v. Microsoft*, the court analyzed the admissibility of "e-mail chains." 2002 WL 649951 (D.D.C. Apr. 12, 2002). The court held that an e-mail prepared by an employee did not qualify as a business record because, while it may have been the regular practice of the employee to send an e-mail following the receipt of a phone call that summarized the call, there had been no showing that it was the regular practice of the employer to require that the employee make and maintain such e-mails. *Id.* at *9. The court was particularly careful in analyzing the hearsay issues associated with e-mail chains involving multiple employees of the same employer. It held that to establish a proper foundation, the proponent would have to show that when the source of the information related in the e-mail is someone other than the maker of the e-mail, that the source, the maker "as well as every other participant in the chain producing the record are, acting in the regular course of [the] business." *Id.* at *14. If this showing is made, the court ruled, then the multiple levels of hearsay in the e-mail chain are covered by Rule 803(6). However, "[i]f the source of the information is an outsider, Rule 803(6) does not, by itself, permit the admission of the business record. The outsider's statement must fall within another hearsay exception to be admissible because it does not have the presumption of accuracy that statements made during the regular course of business have." *Id.* at *14. The court also excluded another e-mail chain for failure of the proponent to establish a proper foundation, saying "[p]laintiffs have not established the requisite foundation that the multiple authors of these e-mails each composed their portion of the document in the course of regularly conducted business activity and that it was the regular practice of RealNetworks to compose such e-mail correspondence. Moreover, the multiple authors and forwarded nature of the e-mails undercuts the reliability of the information contained therein." *Id.* at *19.

Similarly, in *Rambus Inc. v. Infineon Tech. AG*, the Court critically analyzed the admissibility

of e-mail under the business record exception to the hearsay rule. 348 F. Supp. 2d 698, 706 (E.D. Va. 2004). Certain exhibits objected to by the defendant were e-mail chains prepared at least in part by persons outside of the business entity that maintained the e-mail as part of its records, and which was seeking their admissibility as business records. The court noted that there was "not a requirement that the records have been prepared by the entity that has custody of them, as long as they were created in the regular course of some [other] entity's business.'" *Id.* (quoting WEINSTEIN, at § 803.08[8][a]). The court added "[h]owever, it also is true that: To satisfy Rule 803(6) each participant in the chain which created the record–from the initial observer-reporter to the final entrant– must generally be acting in the course of the regularly conduct[ed] business. *Id.* at 707. If some participant is not so engaged, some other hearsay exception must apply to that link of the chain." *Id.* at 706.

In contrast to the demanding approach taken in *Rambus* and *New York v. Microsoft*, the court in *United States v. Safavian* took a more flexible approach to the admissibility of e-mail chains. 435 F. Supp. 2d 36, 40-41 (D.D.C. 2006). The defendant objected to the admissibility of e-mail chains, arguing that they were not trustworthy because they contained e-mails embedded within e-mails. The court overruled this objection, stating:

> [t]he defendant's argument is more appropriately directed to the weight the jury should give the evidence, not its authenticity. While the defendant is correct that earlier e-mails that are included in a chain–either as ones that have been forwarded or to which another has replied–may be altered, this trait is not specific to e-mail evidence. It can be true of any piece of documentary evidence, such as a letter, a contract or an invoice . . . . The *possibility* of alteration does not and cannot be the basis for excluding e-mails as unidentified or unauthenticated as a matter of course . . . .We live in an age of technology and computer use where e-mail communication now is a normal and frequent fact for the majority of the nation's population and is of particular importance in the professional world . . . . Absent specific evidence showing alteration, however, the Court will not exclude any embedded e-mails because of the mere possibility that it can be done."

Id. at 41. Notably, the court did not engage in the demanding business records exception analysis that was done by the courts in *Rambus* and *New York v. Microsoft*.

Perhaps the most demanding analysis regarding the admissibility of electronic evidence under the business record exception to the hearsay rule appears in *In Re Vee Vinhnee*, 336 B.R. at 445. In this case the appellate bankruptcy panel upheld the trial bankruptcy judge's exclusion of electronic business records, observing that "early versions of computer foundations [accepted by courts] were too cursory, even though the basic elements [of the business records exception] covered the ground." The court held that the proponent of an electronic business record was required to show that the paperless electronic record retrieved from its computer files was the same one as originally had been entered into its computer, noting that the "focus is not on the circumstances of the creation of the record, but rather on the circumstances of the preservation of the record during the time it is in the file so as to assure that the document being proffered is the same as the document that originally was created." *Id*. at 444. It added "[t]he logical questions extend beyond the identification of the particular computer equipment and programs used. The entity's policies and procedures for the use of the equipment, database, and programs are important. How access to the pertinent database is controlled and, separately, how access to the specific program is controlled are important questions. How changes in the database are logged or recorded, as well as the structure and implementation of backup systems and audit procedures for assuring the continuing integrity of the database, are pertinent to the questions of whether records have been changed since their creation." *Id*. at 445. The court reasoned that the "complexity of ever-developing computer technology necessitates more precise focus," because "digital technology makes it easier to alter text of documents that have been scanned into a database, thereby increasing the importance of audit procedures designed to assure the continuing integrity of the records." *Id*.

In contrast to the demanding approach taken in *In Re Vee Vinhnee*, many other courts have admitted electronic business records under a much more relaxed standard. *See, e.g.*, *United States v. Kassimu*, 2006 WL 1880335 (5th Cir. 2006) (Establishing the foundation for a computer generated business record did not require the maker of the record, or even a custodian, but only a witness qualified to explain the record keeping system of organization.); *United States v. Fuji*, 301 F.3d 535 (7th Cir. 2002) (holding that computerized check-in and reservation records were admissible as business records on a showing that the data reflected in the printouts was kept in the ordinary course of the business); *Sea Land*, 285 F.3d 808 (holding that copy of electronic bill of lading had been properly admitted as a business record because it had been produced from the same electronic information that had been contemporaneously generated when the parties entered into their contract. The court noted that "it is immaterial that the business record is maintained in a computer rather than in company books." (citation omitted)); *Wapnick v. Commissioners of Internal Revenue*, T.C. Memo. 2002-45, (T.C. 2002)(computerized accounting records were admissible as business records because foundation was established by IRS agents who compared the data in the computer records with information in the company's tax returns, bank statements, and by contacting clients of the company to verify information in the computerized records).

The lesson to be taken from these cases is that some courts will require the proponent of electronic business records or e-mail evidence to make an enhanced showing in addition to meeting each element of the business records exception. These courts are concerned that the information generated for use in litigation may have been altered, changed or manipulated after its initial input, or that the programs and procedures used to create and maintain the records are not reliable or accurate. Others will be content to view electronic business records in the same light as traditional "hard copy" records, and require only a rudimentary foundation. Unless counsel knows what level

of scrutiny will be required, it would be prudent to analyze electronic business records that are essential to his or her case by the most demanding standard. The cases further suggest that during pretrial discovery counsel should determine whether opposing counsel will object to admissibility of critical documents. This can be done by requesting a stipulation, or by propounding requests for admission of fact and genuineness of records under FED. R. CIV. P. 36. If it is known that opposing counsel will object, or refuses to stipulate, or denies a Rule 36 request to admit genuineness, then the lawyer intending to introduce the electronic business record should be prepared to establish the business record exception under the most demanding standard required, to avoid exclusion of the evidence.

Rule 803(8) Public Records.

In addition to the above described hearsay exceptions, courts have found that electronic records also met the requirements of the public records exception under Rule 803(8):

> (8) Public records and reports. Records, reports, statements, or data compilations, in any form, of public offices or agencies, setting forth (A) the activities of the office or agency, or (B) matters observed pursuant to duty imposed by law as to which matters there was a duty to report, excluding, however, in criminal cases matters observed by police officers and other law enforcement personnel, or (C) in civil actions and proceedings and against the Government in criminal cases, factual findings resulting from an investigation made pursuant to authority granted by law, unless the sources of information or other circumstances indicate lack of trustworthiness.

Furthermore, "[j]ustification for the exception is the assumption that a public official will perform his duty properly, and the unlikelihood that he will remember details independently of the record." FED. R. EVID. 803(8) advisory committee's note. Moreover, "[s]ince the assurances of accuracy are generally greater for public records than for regular business records, the proponent is usually not required to establish their admissibility through foundation testimony . . . . The burden of proof concerning the admissibility of public records is on the party opposing their introduction."

WEINSTEIN at § 803.10[2]. Courts have applied this deferential standard of admissibility for electronic public records. *See, e.g., EEOC v. E.I. DuPont De Nemours and Co.*, 2004 WL 2347556 (holding that table of information compiled by U.S. Census Bureau was admissible as an exception to the hearsay rule as a public record under Rule 803(8), and rejecting claims that the posting of data on the Census Bureau's website rendered it untrustworthy); *Lester v. Nastsios*, 290 F. Supp. 2d 11 (D.D.C. 2003) (admitting e-mail of public agency, and noting that "[r]ecords of public agencies such as those challenged by plaintiff are generally admissible ... under FED. R. EVID. 803(8)."); *United States v. Oceguerra*, 70 Fed. Appx. 473 (9th Cir. 2003) (Court held that trial court properly admitted computerized records of Treasury Enforcement Communications System as public records under Rule 803(8) because documents falling under the public records exception are presumed to be trustworthy, and the burden is on the party challenging the records to establish untrustworthiness.)

Rule 803(17) Market Reports, Commercial Publications.

Rule 803(17) recognizes as an exception to the hearsay rule:

> (17) Market reports, commercial publications. Market quotations, tabulations, lists, directories, or other published compilations, generally used and relied upon by the public or by persons in particular occupations.

This exception covers "lists, etc., prepared for the use of a trade or profession . . . newspaper market reports, telephone directories, and city directories. The basis of trustworthiness is general reliance by the public or by a particular segment of it, and the motivation of the compiler to foster reliance by being accurate." FED. R. EVID. 803(17) advisory committee's note; WEINSTEIN at § 803.19[1].[53]

---

[53] [T]he admissibility of market reports and commercial publications under Rule 803(17) is predicated on the two factors of necessity and reliability. Necessity lies in the fact that if this evidence is to be obtained it must come from the compilation, since the task of finding every person who had a hand in making the report or list would be impossible. Reliability is assured because the compilers know that their

At least one court has admitted electronically stored compilations and directories under Rule 803(17). *Elliott Assoc. L.P. v. Banco de la Nacion*, 194 F.R.D. 116, 121 (S.D.N.Y. 2000) (finding that plaintiff's expert report properly relied on prime rates of interest obtained from Federal Reserve Board website because they were reliable under Rule 803(17)).

A final observation needs to be made regarding hearsay exceptions and electronic evidence. Rule 802 generally prohibits the admission of hearsay unless one of the exceptions in Rules 803, 804 or 807 apply. What, then, is the effect of hearsay evidence that is admitted without objection by the party against whom it is offered? The general rule is that despite Rule 802, if hearsay is admitted without objection it may be afforded its "natural probative effect, as if it were in law admissible." *New York v. Microsoft*, 2002 WL 649951 ("[I]n this country the general rule supported by overwhelming weight of authority is that where ordinarily inadmissible hearsay evidence is admitted into evidence without objection it may properly be considered and accorded its natural probative effect, as if it were in law admissible."; 3 MICHAEL H. GRAHAM, HANDBOOK OF FEDERAL EVIDENCE § 802.1 (5th ed. 2001) ("In the absence of an objection to hearsay 'the jury may consider [the hearsay] for whatever natural value it may have; such evidence is to be given its natural probative effect as if it were in law admissible.'" (citation omitted)). This underscores the need to pay attention to exhibits offered by an opponent, as much as to those records that you need to introduce. A failure to raise a hearsay objection means that the evidence may be considered for whatever probative value the finder of fact chooses to give it.

In summary, when analyzing the admissibility of ESI for hearsay issues, counsel should address each step of the inquiry in order: does the evidence contain a statement, made by a person,

---

work will be consulted; if it is inaccurate, the public or the trade will cease consulting their product." (citation omitted)).

which is offered for its substantive truth, but which does not fall into the two categories of statements identified in 801(d)(1)(A) and 801(d)(2). If, as a result of this analysis, a determination is made that the evidence is hearsay, then it is inadmissible unless it covered by one of the exceptions found in Rules 803, 804 and 807.

If ESI has cleared the first three hurdles by being shown to be relevant, authentic, and admissible under the hearsay rule or an exception thereto, it must also be admissible under the original writing rule before it can be admitted into evidence or considered at summary judgment.

The Original Writing Rule, Rules 1001-1008

The next step in evaluating the admissibility of electronic evidence is to analyze issues associated with the original writing rule, which requires an original or duplicate original to prove the contents of a writing, recording or photograph unless secondary evidence is deemed acceptable.[54] *See* FED. R. EVID. 1001-08. The best way to understand the rule is to appreciate its structure. Rule 1001 contains the key definitions that animate the rule: "original," "duplicate," "writing," "recording," and "photograph." The substantive requirements of the original writing rule are succinctly provided by Rule 1002, which mandates that "[t]o prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required, except as otherwise provided in these rules or by Act of Congress." It is Rule 1002 that gives the rule its modern name, the "original writing rule,"

[54] Traditionally the rule has been referred to as the "Best Evidence Rule," which is a misleading title. The rule is more accurately is referred to as the "Original Writing Rule" because it does not mandate introduction of the "best" evidence to prove the contents of a writing, recording or photograph, but merely requires such proof by an "original," "duplicate" or, in certain instances, by "secondary evidence"–any evidence that is something other than an original or duplicate (such as testimony, or a draft of a writing to prove the final version, if no original or duplicate is available." FED. R. EVID. 1001 advisory committee's note; RICE at 190 ("Article X of the Federal Rules of Evidence codified the common law best evidence rule, terming it instead the original writing rule.").

as it requires the original to prove the contents of a writing, recording or photograph, except as excused by the remaining rules in Article X of the rules of evidence. As will be seen, the key to the rule is to determine when "the contents" of a writing, recording or photograph actually are being proved, as opposed to proving events that just happen to have been recorded or photographed, or those which can be proved by eyewitnesses, as opposed to a writing or recording explaining or depicting them. Rule 1003 essentially provides that duplicates are co-extensively admissible as originals, unless there is a genuine issue as to the authenticity of the original, or the circumstances indicate that it would be unfair to admit a duplicate in lieu of an original. *People v. Huehn*, 53 P.3d 733, 738 (Colo. Ct. App. 2002) (duplicates of computer generated bank records admissible to the same extent as an original absent unfairness or lack of authenticity). Because of Rule 1003, duplicates are more often admitted into evidence than originals. RICE at 192 ("As a practical matter, Fed. R. Evid. 1003 has eliminated best evidence objections. Copies from the pages of books, treatises, and the other papers are now introduced in place of the entire volume because photocopies of originals are now admissible as if they were the original."). Rule 1004 is the primary rule that identifies when secondary evidence is admissible. As a practical matter, "secondary evidence" is any proof of the contents of a writing, recording or photograph other than an original or duplicate. Examples include testimony from the author of the writing, or someone who read it, earlier drafts, copies, or an outline used to prepare the final. Rule 1005 describes how to prove the contents of public records, since it is obvious that something other than the original must be used. Rule 1006 permits introduction into evidence of written or testimonial summaries of voluminous writings, recordings or photographs, provided the original or duplicates from which the summaries were prepared were made available to the adverse party at a reasonable time in advance of trial for examination or copying. Thus, Rule 1006 is an example of secondary evidence. Rule 1007 allows

the proof of the contents of a writing, recording or photograph by the deposition or testimony of a party opponent, without having to account for the nonproduction of the original. This is another form of secondary evidence. The final rule in Article X of the Federal Rules of Evidence is Rule 1008. It is a specialized application of Rule 104(b)—the conditional relevance rule—and sets forth what must happen when there is a dispute regarding whether there ever was a writing, recording, or photograph, or when there are conflicting versions of duplicates, originals, or secondary evidence offered into evidence. In such instances, as in Rule 104(b), the jury decides the factual dispute. FED. R. EVID. 1008 advisory committee's note.

It has been acknowledged that the original writing rule has particular applicability to electronically prepared or stored writings, recordings or photographs. One respected commentator has observed:

> Computer-based business records commonly consist of material originally produced in a computer (e.g. business memoranda), data drawn from outside sources and input into the computer (e.g. invoices), or summaries of documents (e.g. statistical runs). The admissibility of computer-based records "to prove the content of a writing" is subject to the best evidence rule set out in Rule 1002. The rule generally requires the original of a writing when the contents are at issue, except that a "duplicate" is also admissible unless a genuine issue is raised about its authenticity. A duplicate includes a counterpart produced by "electronic re-recording, which accurately reproduces the original." Courts often admit computer-based records without making the distinction between originals and duplicates.

WEINSTEIN at § 900.07[1][d][iv] (citation omitted).

When analyzing the original writing rule as it applies to electronic evidence, the most important rules are Rule 1001, containing the definitions; Rule 1002, the substantive original writing rule; Rule 1004, the "primary" secondary evidence rule; Rule 1006, the rule permitting summaries to prove the contents of voluminous writings, recordings and photographs; and Rule 1007, allowing proof of a writing, recording or photograph by the admission of a party opponent.

Rule 1001 states:

> For purposes of this article the following definitions are applicable:
>
> (1) Writings and recordings. "Writings" and "recordings" consist of letters, words, or numbers, or their equivalent, set down by handwriting, typewriting, printing, photostating, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation.
> (2) Photographs. "Photographs" include still photographs, X-ray films, video tapes, and motion pictures.
> (3) Original. An "original" of a writing or recording is the writing or recording itself or any counterpart intended to have the same effect by a person executing or issuing it. An "original" of a photograph includes the negative or any print therefrom. If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an "original."
> (4) Duplicate. A "duplicate" is a counterpart produced by the same impression as the original, or from the same matrix, or by means of photography, including enlargements and miniatures, or by mechanical or electronic re-recording, or by chemical reproduction, or by other equivalent techniques which accurately reproduces the original.

It is apparent that the definition of "writings, recordings and photographs" includes evidence that is electronically generated and stored. *See* FED. RULE EVID. 1001 advisory committee's note ("Traditionally the rule requiring the original centered upon accumulations of data and expressions affecting legal relations set forth in words and figures. This meant that the rule was one essentially related to writings. Present day techniques have expanded methods of storing data, yet the essential form that the information ultimately assumes for useable purposes is words and figures. Hence, the considerations underlying the rule dictate its expansion to include computers, photographic systems, and other modern developments."). It further is clear that under Rule 1001(3) the "original" of information stored in a computer is the readable display of the information on the computer screen, the hard drive or other source where it is stored, as well as any printout or output that may be read, so long as it accurately reflects the data. WEINSTEIN at § 900.07[1][d][iv]; RICE at 194; *Laughner v. State*, 769 N.E.2d 1147, 1159 (Ind. Ct. App. 2002) (ruling that content of internet chat room

communications between defendant and undercover police officer that officer "cut-and-pasted" into a word processing program were originals under state version of original writing rule). Moreover, if a computer record accurately reflects the contents of another writing, and was prepared near the time that the original writing was prepared, it may qualify as an original under Rule 1001. *In re Gulph Woods Corp*., 82 B.R. 373, 377 (Bankr. E.D. Pa.. 1988)[55]. *See also* WEINSTEIN at § 900.07[1][d][iv]. Finally, as already noted, as a result of Rule 1003, the distinction between duplicates and originals largely has become unimportant, as duplicates are co-extensively admissible as originals in most instances.

Once the definitions of the original writing rule are understood, the next important determination is whether the rule applies at all. Rule 1002 answers this question. It provides: "To prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required, except as otherwise provided in these rules or by Act of Congress." As the advisory committee's note to Rule 1002 makes clear:

> Application of the rule requires resolution of the question whether contents are sought to be proved. Thus an event may be proved by non-documentary evidence, even though a written record of it was made. If, however, the event is sought to be proved

---

55

"In today's commercial world, a single transaction often generates successive entries of the same information in separately prepared writings. Though the purposes of these separate records may be different, a computerized business record, prepared simultaneously with or within a reasonable time period of the written record, and containing the same or similar information, would appear to be no less an 'original' than a handwritten record. However, it seems equally clear that where a written record, prepared prior to the computer record, contains a more detailed and complete description of the transaction than that contained in the computer record, the proponent of the evidence should be required to produce the more detailed record, or account for its nonproduction under F.R.E. 1004. Similarly, where a computerized record appears to be nothing more than a summary of a more detailed written record, the written record should be produced except where the requirements of F.R.E. 1006 have been satisfied." (citations omitted).

> by the written record, the rule applies. For example, payment may be proved without producing the written receipt which was given. Earnings may be proved without producing books of account in which they are entered. Nor does the rule apply to testimony that books or records have been examined and found not to contain any reference to a designated matter.
>
> The assumption should not be made that the rule will come into operation on every occasion when use is made of a photograph in evidence. On the contrary, the rule will seldom apply to ordinary photographs . . . . On occasion, however, situations arise in which contents are sought to be proved. Copyright, defamation, and invasion of privacy by photograph or motion picture falls into this category. Similarly, as to situations in which the picture is offered as having independent probative value, e.g. automatic photograph of bank robber, photograph of defendant engaged in indecent act.

FED. R. EVID. 1002, advisory committee's note (citations omitted); *see also* WEINSTEIN at § 1002.05[1] ("The best evidence rule only applies when the writing, recording or photograph is being introduced 'to prove the content of a writing, recording or photograph. The rule is inapplicable when content is not at issue.")(citing FED. R. EVID. 1002)). Whether the content is at issue is determined on a case-by-case basis. *Id*. For example, proof that someone is married may be made by the testimony of a witness to the ceremony. The marriage license is not required. However, the rule applies if the only proof of the marriage is by the record itself. Similarly, someone who heard a politician give a speech may testify to what was said without the video recording of the speech, because the content of the recording is not at issue. In contrast, if the only way to prove the content of the speech is by the video, because there are no witnesses available to testify, the rule would apply to the video recording.

Rule 1002 also does not apply when an expert testifies based in part on having reviewed writings, recordings or photographs, because Rule 703 allows an expert to express opinions based on matters not put into evidence. FED. R. EVID. 1002 advisory committee's note; WEINSTEIN at § 1002.05 [1] ("The best evidence rule does not apply when an expert resorts to material as a basis for an

opinion."). Finally, when the contents of writings, recordings or photographs merely are collateral to the case, meaning they are not "closely related to a controlling issue" in a case, Rule 1002 does not apply, and secondary evidence may be used to prove their contents. FED. R. EVID. 1004(4). In contrast, proving legal transactions, such as wills, contracts, and deeds commonly do involve the best evidence rule because the documents themselves have the central legal significance in the case. WEINSTEIN at § 1002.05[2].

An example of when the original writing rule did apply to electronic evidence is *Laughner v. State*, 769 N.E.2d 1147 (Ind. Ct. App. 2002), *abrogated on other grounds by Farjardo v. State*, 859 N.E.2d 1201 (Ind. 2007). Laughner was charged with attempted child solicitation. To prove the crime, the state offered printouts of instant message chats between the defendant and an undercover police officer posing as a thirteen year old boy. The police officer "cut-and-pasted" the text of the text messages from the internet chat room into a word processing program, and the printouts that were introduced into evidence were prepared from that program. The defendant objected (citing the state version of the original writing rule, which was identical to the federal version), arguing that the printouts were not the "original" of the text of the chat room communications. The appellate court agreed that the state was proving the content of a writing, and that the original writing rule required an original, but found that the printout was an original, reasoning:

> Evidence Rule 1002, the 'best evidence' rule, requires an 'original' in order to prove 'the content' of a writing or recording. However, Evidence Rule 1001(3) provides that when 'data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately is an "original." According to [the police officer] he saved the conversations with Laughner after they were concluded, and the printout document accurately reflected the content of those conversations. Therefore, the printouts could be found to be the 'best evidence' of the conversations [between the defendant and the officer].

Laughner, 769 N.E.2d at 1159.

It is important to keep in mind that failure to properly object to the introduction of evidence in violation of the original writing rule likely will result in a waiver of the error on appeal. WEINSTEIN at § 1002.04[5][a] ("Procedural safeguards adopted by federal courts also militate against an overtechnical application of the best evidence rule. For example, an appellant's failure to properly raise an objection to the best evidence rule at trial will result in waiver of the error on appeal."); *see also State v. Braidic*, 2004 WL 52412 (Wash. Ct. App. 2004) (Defendant was convicted of rape and other sex offenses with minor. At trial, victim's mother testified, without objection, to content of chat room text messages between defendant and victim. Appellate court noted applicability of original writing rule to require original to prove the contents of the chat room records, but found that defense counsel's failure to object did not constitute ineffective assistance of counsel). Counsel need to insure that a timely objection is made to attempts to prove the contents of electronic writings, recordings or photographs in violation of the original writing rule, otherwise waiver of the error is the probable consequence.

Rule 1004 identifies four circumstances in which secondary evidence may be introduced instead of an original. The rule provides:

> The original is not required, and other evidence of the contents of a writing, recording, or photograph is admissible if–
>
> (1) Originals lost or destroyed. All originals are lost or have been destroyed, unless the proponent lost or destroyed them in bad faith; or
>
> (2) Original not obtainable. No original can be obtained by any available judicial process or procedure; or
>
> (3) Original in possession of opponent. At a time when an original was under the control of the party against whom offered, that party was put on notice, by the pleadings or otherwise, that the contents would be a subject of proof at the hearing, and that party does not produce the original at the hearing; or
>
> (4) Collateral matters. The writing, recording, or photograph is not closely related to

a controlling issue.

The first example may be particularly suited for electronic evidence. Given the myriad ways that electronic records may be deleted, lost as a result of system malfunctions, purged as a result of routine electronic records management software (such as the automatic deletion of e-mail after a set time period) or otherwise unavailable means that the contents of electronic writings may have to be proved by secondary evidence.[56] Indeed, at least one court has recognized that the "tenuous and ethereal nature of writings posted in internet chat rooms and message boards means that in all likelihood the exceptions [to the original writing rule that permit secondary evidence] would . . . [apply]." *Bidbay.com, Inc. v. Spry*, 2003 WL 723297 (Cal. App. 2004)(unpublished opinion); *People v. Huehn*, 53 P.3d 733, 738 (Colo. Ct. App. 2002) (holding that trial court did not abuse discretion in admitting computer generated bank records that contained listing of ATM transactions prepared by another company that bank retained to process ATM transactions. The court noted that the Colorado version of Rule 1004(1) permitted secondary evidence of the records provided they were not lost or destroyed in bad faith).

Additionally, Rule 1004 permits proof of the contents of a writing, recording or photograph by secondary evidence when the proponent of the evidence is unable to obtain an original through use of legal process, or when the original is in the possession or control of an adverse party that has actual or inquiry notice of the contents that the proponent intends to introduce the evidence. In the later

[56] *See,* for example. newly revised Fed. R. Civ. P. 37(f), which creates a limited "safe harbor" from sanctions if electronically stored information is not preserved as a result of the routine good faith operation of an electronic records management system. Sanctions may be imposed if the court finds the presence of "extraordinary circumstances" or if it determines that the loss of the ESI was the result of non-routine loss or destruction, or action taken in the absence of good faith. The new rule evidences the widespread recognition that electronically stored information is not infrequently lost or destroyed.

circumstance, as the advisory committee's note to Rule 104(3) points out, "[a] party who has an original in his control has no need for the protection of the [original writing] rule if put on notice that proof of contents will be made. He can ward off secondary evidence by offering the original."

Finally, Rule 1004(4) permits proof of the contents of writings, recordings of photographs by secondary evidence if they relate to "collateral matters," defined as "not closely related to a controlling issue" in the case. The advisory committee's note to Rule 1004(4) candidly acknowledges that this is a nebulous standard, stating "[w]hile difficult to define with precision, situations arise in which no good purpose is served by production of the original." *See also* WEINSTEIN at § 1004.40 ("[t]he distinction between controlling and collateral issues can be an exasperating one. The term 'collateral' is elusive and vague. It cannot be defined conceptually, only pragmatically: balancing the importance of the document against the inconvenience of compelling its production, is the rule worth enforcing?")(citation omitted). An example illustrates. A doctor testifying as an expert in a personal injury case can testify that she is licensed to practice medicine in a state without having to produce the license itself. However, if a defendant is charged with practicing medicine without a license, his testimony alone that he has a license from the state will not be accepted, as the license is closely related to a controlling issue in the case.

Rule 1006 recognizes another source of secondary evidence to prove the contents of writings, recordings, or photographs, stating:

> The contents of voluminous writings, recordings, or photographs which cannot conveniently be examined in court may be presented in the form of a chart, summary, or calculation. The originals, or duplicates, shall be made available for examination or copying, or both, by other parties at reasonable time and place. The court may order that they be produced in court.

The advisory committee's note recognizes that Rule 1006 is one of necessity, as the "admission of summary of voluminous books, records, or documents offers the only practicable means of making

their contents available to judge and jury." A number of observations may be made about the use of summaries under Rule 1006. First, as the rule expressly states, the writings, recordings or photographs to be summarized must be voluminous. WEINSTEIN at § 1006.03 ("Charts, summaries or calculations are, however, inadmissible when the content being proved is neither voluminous or complicated.")(citations omitted). Second, although the rule is silent on the nature of the summary, the prevailing view is that it may be either written, or testimonial. *Id*. at § 1006.05[2] ("[s]ummary evidence need not be an exhibit, but may take the form of a witness's oral testimony."). Third, the majority view is that the summaries themselves constitute the evidence of the contents of the materials summarized, rather than the underlying writings, recordings or photographs. *Id*. at § 1006.04[1] ("[t]he majority rule is that the summary itself is the evidence to be considered by the factfinder when the underlying documents are voluminous and the other requirements of Rule 1006 are met. Other decisions, however, have held that Rule 1006 summaries were not evidence, and that the jury should be so instructed."). Fourth, if the summaries are accepted as the evidence of the materials summarized, they function as the equivalent of a special exception to the hearsay rule. *Id*. at § 1006.05[4] ("Rule 1006 should be regarded as a special exception to the hearsay rule."); RICE at 197-98 (Recognizing that summaries of voluminous materials that are introduced to prove the content of the summarized material creates a hearsay problem. The author suggests that the residual hearsay rule, Rule 807, is an exception that may apply to overcome this problem). Fifth, the writings, recordings and photographs that are summarized must be made available to the adverse party for examination or copying reasonably in advance of the use of the summary, a requirement that originates from Rule 1006 itself, regardless of whether the adverse party has served a request for production of documents under FED. R. CIV. P. 34. WEINSTEIN at § 1006.06[1] ("the originals or duplicates of voluminous writings, recordings, or photographs must be made available for examination or copying at a

reasonable time or place in order for summary evidence to be admissible. The right to examine the underlying records is absolute. Thus, the records must be made available whether or not the opposing party makes a discovery request for inspection."). Sixth, the underlying materials from which the summaries are made must themselves be admissible into evidence. *Id*. at § 1006.06[3] ("Charts, summaries and calculations are only admissible when based on original or duplicate materials that are themselves admissible evidence.").

Because the production of electronically stored information in civil cases frequently is voluminous, the use of summaries under Rule 1006 is a particularly useful evidentiary tool, and courts can be expected to allow the use of summaries provided the procedural requirements of the rule are met. *See, e.g., Wapnick v. Comm'r of Internal Revenue, T.C. Memo*. 2002-45, (T.C. 2002) (holding that summaries of voluminous computer records were admissible under Rule 1006 even though they were prepared in anticipation of litigation, because the underlying documents had been admitted into evidence and reasonably had been made available to the opposing party to inspect).

Rule 1007 identifies another, though little used, way in which secondary evidence may be used to prove the contents of electronically prepared or stored information. It provides that the:

> [c]ontents of writings, recordings, or photographs may be proved by the testimony or deposition of the party against whom offered or by that party's written admission, without accounting for the nonproduction of the original.

On its face this rule is limited to admissions by a party opponent regarding the content of a writing, recording or photograph. Use of the word "admission" refers to any of the types of admissions covered by Rule 801(d)(2), which includes admissions by a representative, agent, employee or co-conspirator that meets the requirements of Rule 801(d)(2) for each of these types of admissions. WEINSTEIN at §§ 1007.03[1], 1007.06. It does not require that any showing be made that the writing, recording or photograph is lost or otherwise unavailable. *Id*. at § 1007.04[1]. Further, the rule

expressly limits the types of admissions that may be used to prove the contents of writings, recordings or photographs to those obtained during in court testimony, during a deposition, or by the adverse party's written admission.[57] *Id*. at § 1007.04. An adverse party's answers to federal rule of civil procedure Rule 33 interrogatories or a Rule 36 request to admit the genuineness of documents would meet the provisions of Federal Rule of Evidence 1007 regarding a "written admission." *Id*. at § 1007.07 ("[A]n adverse party's responses to written interrogatories made pursuant to Federal Rule of Civil Procedure 33 are admissible to prove content. Similarly, an adverse party's responses to requests for admissions made pursuant to Federal Rule of Civil Procedure 36, are admissible to prove contents.").

Because Rule 1007 so seldom is used or discussed in cases, most lawyers are unaware of it. However, given the frequency with which deponents are asked questions about the content of writings, recordings and photographs, it is prudent to remember that if the deponent is a person whose testimony would qualify as an admission under any of the five varieties recognized by Rule 801(d)(2), then the deposition testimony may be admitted to prove the contents of the writings, recordings and photographs described. The same is true for written responses to FED. R. CIV. P. 33 and 36 discovery that asks for a description of the contents of a writing, recording or photograph. The need is obvious, therefore, to insure that any characterization of the contents of a writing, recording or photograph that

---

[57] However, despite the limitation in Rule 1007 to testimonial or written admissions of a party opponent, a non-testimonial oral admission by a party opponent would still be admissible as secondary evidence to prove the contents of a writing, recording or photograph under Rule 1004 if the writing, recording or photograph was lost of destroyed, absent bad faith, beyond the reach of court ordered production, in the possession, custody of control of the adverse party, or if the writing, recording or photograph was not closely related to a controlling issue in the litigation. FED. R. EVID. 1007 advisory committee's note ("The limitation [of] Rule 1007 to testimonial or written admissions], of course, does not call for excluding evidence of an oral admission when nonproduction of the original has been accounted for and secondary evidence generally has become admissible."); WEINSTEIN at § 1007.03[1].

could fall within Rule 1007 be accurate.

Rule 1008 is the last of the rules in Article X of the rules of evidence. It states:

> When the admissibility of other evidence of contents of writings, recordings, or photographs under these rules depends upon the fulfillment of a condition of fact, the question whether the condition has been fulfilled is ordinarily for the court to determine in accordance with the provisions of rule 104. However, when an issue is raised (a) whether the asserted writing ever existed, or (b) whether another writing, recording, or photograph produced at the trial is the original, or (c) whether other evidence of contents correctly reflects the contents, the issue is for the trier of fact to determine as in the case of other issues of fact.

This rule is a specialized application of Rule 104(b), and it allocates responsibility between the trial judge and the jury with respect to certain preliminary matters affecting the original writing rule. As the advisory committee's note to Rule 1008 states:

> Most preliminary questions of fact in connection with applying the rule preferring the original as evidence of contents are for the judge, under the general principles announced in Rule 104[a]. Thus, the question whether the loss of the originals has been established, or of the fulfillment of other conditions specified in Rule 1004, supra, is for the judge. However, questions may arise which go beyond the mere administration of the rule preferring the original and into the merits of the controversy . . . The latter portion of [Rule 1008] is designed to insure treatment of theses situations as raising jury questions. The decision is not one for uncontrolled discretion of the jury but is subject to the control exercised generally by the judge over jury determinations. *See* Rule 104(b).

See also WEINSTEIN at § 1008.02[1]-1008.04[5]. Under the rule, the trial judge determines: whether originals have been lost or destroyed under Rule 1004(a), as well as all issues relating to the appropriateness of the proponent's efforts to search for the lost original;[58] whether or not the original is obtainable by judicial process, under Rule 1004(b);[59] whether the original is in the possession,

[58] WEINSTEIN at § 1008.04[3]

[59] *Id.* at § 1008.04[4]

custody or control of the opposing party under Rule 1004(3);[60] and whether the writing, recording or photograph relates to a collateral matter, which removes it from the reach of the original writing rule.[61]

Rule 1008 identifies three issues that are questions for the jury, however: (1) whether the writing, recording or photograph ever existed in the first place; (2) whether some other writing, recording, or photograph that is offered into evidence is in fact the original; and (3) whether "other" (i.e. secondary) evidence of contents correctly reflects the content of the writing, recording or photograph. FED. R. EVID. 1008 advisory committee's note; WEINSTEIN at §1008.05[1]. Counsel need to be aware of the different functions the judge and jury serve as they anticipate how to offer electronic writings, recordings and photographs into evidence. Given the challenges that often are associated with the authentication of electronically created or stored evidence, it is not unlikely that there will be disputes of fact regarding whether an electronic writing ever existed in the first place, if the original cannot be produced and secondary evidence is offered, or when different versions of the same electronic document are offered into evidence by the opposing parties.

In summary, when counsel intend to offer electronic evidence at trial or in support of a motion for summary judgment they must determine whether the original writing rule is applicable, and if so, they must be prepared to introduce an original, a duplicate original, or be able to demonstrate that one of the permitted forms of secondary evidence is admissible. In this case, counsel did not address the original writing rule, despite its obvious applicability given that the e-mail exhibits were closely related to a controlling issue and there were proving the contents of the e-mails themselves.

The final evidentiary issue that must be considered in determining whether electronic evidence

---

[60] *Id.* at § 1008.04[5]

[61] *Id.* at § 1008.04[6]

will be admitted is whether the probative value of the evidence is substantially outweighed by the danger of unfair prejudice, as proscribed under Rule 403 of the federal rules of evidence.

Balancing Probative Value Against the Danger of Unfair Prejudice Under Rule 403

After evaluating the issues associated with relevance, authenticity, hearsay, and the original writing rule, the final step to consider with regard to electronically prepared or stored evidence is the need to balance its probative value against the potential for unfair prejudice, or other harm, under Rule 403 of the Federal Rules of Evidence. This rule states:

> Although relevant, evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence.

FED. R. EVID. 403. The advisory committee note to Rule 403 succinctly explains its function:

> [C]ertain circumstances call for the exclusion of evidence which is of unquestioned relevance. These circumstances entail risks which range all the way from inducing decision on a purely emotional basis, at one extreme, to nothing more harmful than merely wasting time, at the other extreme. Situations in this area call for balancing the probative value of and need for the evidence against the harm likely to result from its admission . . . . 'Unfair prejudice' within its context means an undue tendency to suggest decision on an improper basis, commonly, though not necessarily an emotional one.

See also WEINSTEIN at § 403.02[1][a].[62]

A determination of whether evidence should be excluded under Rule 403 falls within the those made by the court under Rule 104(a), but it is used sparingly. WEINSTEIN at § 403.02[2][a]. Generally,

[62]"Rule 403 recognizes that relevance alone does not ensure admissibility. A cost/benefit analysis must often be employed. Relevant evidence may be excluded if its probative value is not worth the problems that its admission may cause. The issue is whether the search for truth will be helped or hindered by the interjection of distracting, confusing, or emotionally charged evidence."

"[i]f there is doubt about the existence of unfair prejudice, confusion of issues, misleading, undue delay, or waste of time, it is generally better practice to admit the evidence, taking necessary precautions of contemporaneous instructions to the jury followed by additional admonitions in the charge." *Id*. at § 403.02[2][c].

Although Rule 403 may be used in combination with any other rule of evidence to assess the admissibility of electronic evidence, courts are particularly likely to consider whether the admission of electronic evidence would be unduly prejudicial in the following circumstances: (1) When the evidence would contain offensive or highly derogatory language that may provoke an emotional response. *See Monotype Corp.*, 43 F. 3d at 450 (Finding that trial court properly excluded an email from a Microsoft employee under Rule 403 that contained a "highly derogatory and offensive description of . . . [another company's] type director."); (2) When analyzing computer animations, to determine if there is a substantial risk that the jury may mistake them for the actual events in the litigation, *Friend v. Time Manufacturing Co.*, 2006 WL 2135807 at * 7 (D. Ariz. 2006)("Therefore, the question is simply whether the animation accurately demonstrates the scene of the accident, and whether the probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence."); *State v. Sayles*, 662 N.W. 2d 1, 11 (Iowa, 2003) (Appellate court found no error in trial court's admission of computer animation slides showing effects of shaken infant syndrome, finding that trial court properly considered state version of Rule 403, and admitted evidence with a cautionary instruction that the evidence was only an illustration, not a re-creation of the actual crime); (3) when considering the admissibility of summaries of voluminous electronic writings, recordings or photographs under Rule 1006, WEINSTEIN at § 1006.08[3] ("Summary evidence is subject to the balancing test under Rule 403 that weighs the probative value of evidence

against its prejudicial effect."); and (4) In circumstances when the court is concerned as to the reliability or accuracy of the information that is contained within the electronic evidence, *St. Clair v. Johnny's Oyster and Shrimp Inc*., 76 F. Supp. 2d 773 (S.D. Tx. 1999) (Court expressed extreme skepticism regarding the reliability and accuracy of information posted on the internet, referring to it variously as "voodoo information". Although the court did not specifically refer to Rule 403, the possibility of unfair prejudice associated with the admissibility of unreliable or inaccurate information, as well as for confusion of the jury, makes Rule 403 a likely candidate for exclusion of such evidence).

Thus, when a lawyer analyzes the admissibility of electronic evidence, he or she should consider whether it would unfairly prejudice the party against whom it is offered, confuse or mislead the jury, unduly delay the trial of the case, or interject collateral matters into the case . If a lawyer is offering electronic evidence, particularly computer animations, that may draw a Rule 403 objection, he or she must be prepared to demonstrate why any prejudice is not unfair, when measured against the probative value of the evidence. In this case, counsel did not address whether Rule 403 was implicated with respect to the electronic evidence attached to their summary judgment memoranda.

Conclusion

In this case the failure of counsel collectively to establish the authenticity of their exhibits, resolve potential hearsay issues, comply with the original writing rule, and demonstrate the absence of unfair prejudice rendered their exhibits inadmissible, resulting in the dismissal, without prejudice, of their cross motions for summary judgment. The discussion above highlights the fact that there are five distinct but interrelated evidentiary issues that govern whether electronic evidence will be admitted into evidence at trial or accepted as an exhibit in summary judgment practice. Although each of these rules may not apply to every exhibit offered, as was the case here, each still must be

considered in evaluating how to secure the admissibility of electronic evidence to support claims and defenses. Because it can be expected that electronic evidence will constitute much, if not most, of the evidence used in future motions practice or at trial, counsel should know how to get it right on the first try. The Court hopes that the explanation provided in this memorandum order will assist in that endeavor.[63]

May 4, 2007

/S/

PAUL W. GRIMM
CHIEF UNITED STATES MAGISTRATE JUDGE

[63]I acknowledge with gratitude the tireless assistance of two exceptionally talented law student interns, Ms. Puja Gupta and Mr. Ben Peoples, whose assistance in cite checking was invaluable, and my law clerk, Ms. Kathryn Widmayer, who consistently makes the most difficult tasks appear easy.

INTERNATIONAL MUNICIPAL LAWYERS ASSOCIATION



Concurrent Session VIII – Construction Law
Monday, October 19, 2009

Title: **Surfing the E-Discovery Tsunami – An E-Discovery Surfer's Guide to Avoiding Reefs and Wipeouts in Construction and Civil Litigation.**

Presenters: **Roy Cooper**
Senior Vice President
PinnacleOne an ARCADIS company
Middletown, Connecticut

Edwin Levy
Senior Counsel
New York City Law Department
Commercial & Real Estate Litigation
New York, New York

John P. Markovs
Associate County Attorney
Office of the County Attorney
Montgomery County, Maryland

Donald C. Ramsay
Of Counsel
Stinson Morrison Hecker LLP
Overland Park, Kansas

John Rannestad
Senior Consultant
PinnacleOne an ARCADIS company
Middletown, Connecticut

© 2009 International Municipal Lawyers Association. The following informational and educational materials were distributed by the International Municipal Lawyers Association during its 2009 Annual Conference, held October 18-21, 2009 in Miami, Florida. IMLA assumes no responsibility for the policies or positions presented in the materials or for the presentation of its contents.