

# Handling Electronic Discovery

presented by

Robert Gegios

KOHNER, MANN & KAILAS, s.c.  
ATTORNEYS AT LAW

“Discovery, preservation, and production of electronic data is one of the leading legal issues facing not only corporate America but also government.”

Shirley S. Abrahamson, C.J.

*In re John Doe Proceeding*, 272 Wis. 2d 208 (Wis. 2004)  
(Abrahamson, C.J., concurring).

Why Be Concerned?

- Primary Sources of Electronic Discovery
  - Mainframe, PC & lap-top hard drives, databases, email, instant messaging, web servers, and P.D.A.s.
  
- Hidden Sources of Electronic Discovery
  - Deleted files: deletion is not destruction.
  - Metadata: information about document creation and revision.
  - Legacy Data: information left over from old applications.

- Up to 90% of information is now created electronically.
- 35% to 70% of electronic information never reaches hard copy.
- Discovery of e-mail now occurs in the majority of federal civil cases.
- Electronic discovery often involves tremendous cost.

- Federal discovery rules apply equally to the production of electronic evidence. *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421 (S.D.N.Y. 2002).
- Local jurisdictions increasingly require counsel to understand the types of data a client has, and what is required to retrieve that electronic information.
- Failure to produce can result in harsh sanctions: About 65% of sanctions requests are granted.
- Companies often do not know what they possess, and few are prepared to respond adequately.

# The Duty To Preserve

# The Duty to Preserve Evidence:

*Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, (S.D.N.Y. 2003) (*Zubulake IV*):

- The duty to preserve arises when a party reasonably anticipates litigation. See also *Broccoli v Echostar Comms. Corp.*, 229 F.R.D. 506 (D. Md. 2005).
- Duty covers any information:
  - Relevant to the claims or defenses of any party,
  - “relevant to the subject matter,”
  - “reasonably calculated to lead to the discovery of admissible evidence,”
  - “reasonably likely to be requested during discovery,”
  - and/or the “subject of a pending discovery request.”

- Deleted electronic records are discoverable.  
*Dodge, Warren & Peters Ins. Serv. v. Riley*, 130 Cal Rptr. 2d (Cal. App. 2003).
- There are special rules for “key players.”
  - Back-up tapes of “key players” should be preserved.
  - Failure to notify and fully inform key players may result in an order of contempt.  
*Landmark Legal Found. v. EPA*, 272 F. Supp. 2d 70 (D.D.C. 2003).
- The Duty to Preserve is Ongoing Once a "litigation hold" is in place:
  - A party must ensure that all sources of potentially relevant information are placed "on hold."  
*Zubulake v. UBS Warburg LLC*, 2004 WL 1620866 (S.D.N.Y. July 20, 2005) (*Zubulake V*).

# When must a party reasonably anticipate litigation?

- Receipt of a discovery request or the filing of a complaint. *Applied Telelmatics v. Sprint Comms. Co.*, 1996 U.S. Dist. LEXIS 14053 (E.D. Penn).
- A preservation order issues. *Keir v. UnumProvident Corp.*, 2003 U.S. Dist. LEXIS 14422 (S.D.N.Y.).
- Service of a subpoena. *Arthur Anderson LLP v. United States*, 544 U.S. 696 (2005).
- A complainant threatens litigation. *Testa v. Wal-Mart*, 144 F.3d 173 (1st Cir. 1998).
- Attorney requests information concerning a dispute on behalf of a client. *Binzler v. Marriott Int'l Inc.*, 81 F. 3d 1148 (1st Cir. 1996).
- A complaint by an employee to a direct supervisor. *Broccoli v. EchoStar Comms. Corp.*, 229 F.R.D. 506 (D. Md. 2005).
- Receipt of a preservation letter.

## Preservation letters:

- Provide counsel with the means to trigger another's duty to preserve.
- Place the opposing party, or a third party, on notice that electronic discovery will be important in the litigation.
- May circumvent need for a preservation order. *In re Cell Pathways, Inc. Sec. Litig., II*, 203 F.R.D. 189 (E.D. Pa. 2001).
- Letters also allow parties to work out discovery requests without involving the court, consistent with the principles of proposed Fed. R. Civ. P. 26.

- Preservation Letters should:
  - Remind the other party that the rules prohibiting the destruction of evidence apply equally to electronic evidence.
  - Remind the other party that its duty to preserve evidence extends to ceasing data destruction and backup tape recycling policies.
  - State that you believe that the party has electronic information that will be an irreplaceable source of material evidence in the upcoming litigation.
  - Give a focused description of such sources and the types of electronic evidence sought.

# Other Duties of Counsel

## Counsel also have a duty to:

- Learn the nature and contents of electronic information held by a client.
- Advise the client on the legal significance of data retention.
- Advise the client regarding the characteristics of an appropriate disposal policy.
  - Reducing the longevity and scope of retention is not spoliation until “the path to litigation is clear and immediate.” *Hynix Semiconductor v. Rambus Inc.*, 2006 WL 565893) (N.D. Cal.).
  - However, when litigation was anticipated, such a change in practice falls under the crime/fraud exception to privilege. *Rambus Inc. v. Infineon Technologies AG.*, 222 F.R.D. 280 (E.D. Va. 2004).

Counsel also have a duty to:

- Take affirmative action to ensure a client's compliance with preservation requirements.
  - Learn client's document retention policies.
  - Speak with knowledgeable technology personnel.
  - Trial counsel are obligated to identify key players in conjunction with in-house counsel. *Cardenas v. Dorel Juvenile Group Inc.*, 2006 WL 1537394 (D. Kan.).
  - Trial counsel have a duty to ensure that client employees are informed of their preservation obligations, and competently, ethically and diligently comply with them. *Id.* Evidence of active enforcement, including random audits, may be required.
  - Review all documents not only for privilege, but for indications that other unidentified relevant documentation may exist. *Id.*

# Uninformed Review Practices Invite Sanctions

- A lawyer opening a file to review for discovery, or cutting and pasting information, potentially destroys metadata. Such actions, often conducted in an attempt to comply with discovery, likely overwrite or erase file paths, amendment data, etc., which may legally be spoliation.
- Simply collating records may not suffice. Forensic review of duplicated sources, which retains metadata that collation loses, may now be becoming the standard expected.

## An Outline Litigation Plan should be prepared in advance, and include:

- A register of data sources - PDA's, Laptops, home offices, thumb drives, etc.
- What systems, applications and databases has the company used, and when? Is legacy data accessible?
- Key players, where they store data and what applications they have authority to access.
- File-naming and save location rules and enforcement of these.
- On-going routine records management practices.
- A database of employees, ex-employees, and others with access to identified systems for identified time periods.

# Consequences of Failure to Preserve

Failure to preserve electronic evidence can result in the following sanctions:

- Dismissal
- Adverse inference instruction
- Striking of pleadings
- Monetary sanctions
- Default judgment
- Exclusion of expert witness testimony

## Dismissal –

*Kucala Enters. Ltd. v. Auto Wax Co.*, 2003 WL 21230605 (N.D. Ill.):

- Plaintiff ran the “Evidence Eliminator” software program claimed to “clean” computer hard drives of “deadly evidence.”
- The court dismissed the case with prejudice and ordered the plaintiff to pay the defendant’s attorneys’ fees.

## Adverse Inference Instruction –

*Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212  
(S.D.N.Y. 2003) (*Zubulake V*).

- Key player deleted relevant e-mails despite directions from counsel, and never produced potentially relevant information to counsel.
- “If you find that UBS could have produced this evidence, and that the evidence was within its control, and that the evidence would have been material in deciding facts in dispute in this case, you are permitted, but not required, to infer that the evidence would have been unfavorable to UBS.”

## Striking the Pleading –

*QZO, Inc. v. Moyer*, 594 S.E. 2d 541 (S.C. Ct. App. 2004):

- After reformatting his computer, the defendant turned over discovery seven days after temporary restraining order had been issued.
- The lower court imposed sanctions and struck the defendant's answer. This decision was affirmed on appeal.

## Monetary Sanctions –

*Coleman Parent Holdings Inc. v. Morgan Stanley*, 2005 WL 674885 (Fl. Cir. Ct.):

- Defendant certified compliance with plaintiff's discovery requests. Later plaintiff learned of 1,600 undisclosed tapes.
- Jury instructed to consider misconduct in awarding punitive damages. Result: \$850 million punitive and \$604 million in compensatory damages.

*But compare E & J Gallo Winery v. Encana Energy Servs., Inc.*, 2005 WL 3709885 (E.D. Cal.):

- Counsel repeatedly mirrored legitimate discovery motions by the plaintiff, regardless of merit.
- Use of discovery motions as retaliatory weapon to harass and divert the plaintiff will not be tolerated.
- \$102,079 sanction imposed on defendant's lawyers.

## Default Judgment –

*Krumwiede v. Brighton Assocs. LLC.*, 2006 WL 1308629 (N.D. Ill.):

- Plaintiff long resisted handing lap-top to expert.
- Found defendant had used delay to destroy evidence.
- Plaintiff claimed legitimate explanation but placed lap-top with a third party and refused to seek its return.
- Court found he was “hiding the ball,” discerning a pattern of obstruction amounting to blatant contempt.
- Defendant granted judgment on its counterclaims, a trial on the issue of damages, all costs and fees relating to the sanctions motion, and attorney fees for the whole litigation.

- Exclusion of Expert Testimony – *U.S. v. Philip Morris USA, Inc.*, 327 F. Supp. 2d 21 (D.D.C. 2004):
  - Defendant disobeyed preservation order by continuing to erase emails that were sixty days old on a monthly basis for two years after the order was granted.
  - The court barred witnesses that failed to comply with the order for preservation from testifying.
  - \$3 million in sanctions awarded.

# Cost Shifting: Case Law

## Cost-Shifting Case Law

Generally, each party bears its own discovery costs even if it is very costly; however, cost-shifting may be available in some situations if certain tests are satisfied.

- The Marginal Utility Test: the more likely the search will discover critical information, the fairer it is to have the responding party pay costs.
- *McPeck v. Abbott*, 202 F.R.D. 31, 50 (D.D.C. 2001): Court ordered a “sampling” of requested information from back-up tapes: if the sampling produced a significant amount of responsive documents, expanding the search would be appropriate.

## Cost-Shifting Case Law:

*Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421 (S.D.N.Y. 2002):

Eight-factor test that incorporated the Marginal Utility Test:

1. “The less specific the requesting party's discovery demands, the more appropriate it is to shift the costs.”
2. Likelihood of discovering material data.
3. If information is accessible in another format at less expense, costs probably will not shift.
4. If information is currently used in the course of business, this weighs against cost-shifting.
5. If respondent benefits, cost-shifting less justified.
6. Low cost of production weighs against cost-shifting.
7. The relative ability of each party to control its own costs: “place the burden on the party that will decide how expansive the discovery will be.”
8. The relative resources of the parties.

## Cost-Shifting Case Law:

*Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003)(*Zubulake I*):

- Held *Rowe* did not take adequate consideration of Rule 26. The court disregarded two *Rowe* factors:
  - The specificity of request (factor 1).
  - The responding party's purpose for retaining data (factor 4).

## New Seven-Factor Test:

1. Specifically tailored to discover relevant information?
  2. Is the information available from other sources?
  3. Cost of production, compared to amount in controversy.
  4. Cost of production, compared to resources of each party.
  5. Ability and incentive of each party to control costs.
  6. Importance of the issues at stake in the litigation.
  7. Relative benefits to the parties of obtaining the information.
- The Eastern District has adopted the *Zubulake* seven-factor test. *Hagemeyer North American, Inc., v. Gateway Data Sciences Corp.*, 222 F.R.D. 594, 602-03 (E.D. Wis. 2004).

## Cost-Shifting Case Law:

*Zubulake v. UBS Warburg LLC*, 216 F.R.D. 280 (S.D.N.Y. 2003)  
(*Zubulake III*) - addressing sampling ordered in *Zubulake I*

- Cost-shifting is generally “appropriate only when inaccessible data is sought.” Applied the seven factors to the evidence obtained from the sampling.
- Found that relevant data was improperly erased.
- “The cost of accessing those documents may be onerous, and in some cases the parties should split the cost of breaking into the safe. But once the safe is opened, the production of the documents found inside is the sole responsibility of the responding party.”
- Respondent should always bear the cost of reviewing and producing data converted to an accessible form.
  - Producing party has the exclusive ability to control the cost of reviewing the documents.
  - Once the data is in an accessible format and responsive documents located, cost-shifting is no longer appropriate.

## Cost-Shifting Case Law:

*Wiginton v. CB Ellis, Inc.*, 2004 WL 1895122 (N.D. Ill.)

- Addressing the results of a sampling of an inaccessible source (back-up email repository) conducted by an electronic discovery service.
- Plaintiff and the defendant each chose four search terms.

## Applied the *Rowe* and *Zubulake* factors:

- Added a factor: the importance of the requested discovery in resolving the issues of the litigation.
- The “marginal utility factor” is the most important factor, followed by the specificity of the request.
  - “ the more likely it is that relevant information will be discovered, the fairer it is to make the responding party pay for the information.”

# Proposed Amendments to the Federal Rules

## Proposed Amendments to the Fed. R. Civ. P. - Effective December 1, 2006.

- The rule changes are intended to:
  - Ensure focus on electronic discovery issues at the earliest stages of the litigation process: Rules 16 and 26(f) and Rule 26(a)(1).
  - Improve management of discovery of inaccessible data: Rule 26(b)(2).
  - Create procedure for asserting privilege post production: Rule 26(b)(5).
  - Clarify sanctions rules in circumstances not encountered in paper-based discovery: Rule 37.
  - Clarify rules relating to requests for production of electronically stored information: Rules 33 and 34.

## Early Focus on Electronic Discovery

- Aimed at incentivizing early and efficient discovery of electronic information.
- Parties required to discuss any issues relating to electronic discovery during pre-trial conferences, including inaccessible data.
- Parties may agree that privilege may be asserted post production.
- Such agreements may be included in a Rule 16(b) order.

## Rule 26(f) - Pre-Trial Discussion of Inaccessible Data:

- The parties should address the balance between the need to preserve relevant evidence and the risk that material cessation of computer operations could paralyze activities.
- The parties should weigh the burden or cost of obtaining information from different available sources.
- The parties are explicitly directed to discuss the form discovery shall take.
- The discovering party should stipulate a reasonable form; otherwise the respondent must give notice of the forms it intends to utilize.
- Failure to comply with format risks the respondent having to reproduce the information in a second format, at its own cost.
- The requirement to discuss preservation is not a signal for courts to grant preservation orders routinely.

## Inaccessible Data Sources - 26(b)(2)(B):

- Best Practice established as a two-tiered methodology:
  1. Identify information available from accessible sources.
  2. Determine whether it is actually necessary to search any of the harder-to-access sources.
- Respondent identifies sources of electronic information not readily accessible because of undue burden or cost.
- Respondent must identify inaccessible sources not searched or produced, by category and type, sufficient that the requesting party can estimate the cost and probability of finding pertinent information.
- Respondent bears the burden of showing burden or cost.
- Court may still order discovery for “good cause.”

# Sampling of Inaccessible Data Sources - Rule 34(a)(1):

- Subject to burden testing:
  - The specificity of the discovery request.
  - The quantity of information available from other, more readily accessible sources.
  - Did similar information exist in accessible sources but since has been lost before being discovered?
  - Is the information potentially available from another source?
  - Likely materiality of information from the source in question.
  - The importance of the issues in controversy.
  - The resources of the parties.
  - The requestor's willingness to assume all or part of the costs of access.

## Assertion of Privilege Post Production - 26(b)(5)

- Framework designed to enable voluntary agreement on procedures enabling disclosure of electronically-stored information without waiver of privilege.
- Recognition of the significant costs and delays stemming from the need to screen prior to discovery.
- Establishes a default procedure. Where information is disclosed that is properly subject to protection:
  - The party asserting protection may notify recipients, who must then return, destroy, or sequester the information promptly.
  - If the recipient disputes the assertion, the information may be deposited under seal with the court for determination of the claim.

## Sanctions: A Very Limited Safe Haven for Good Faith, Routine Operations - Rule 37(f)

- No safe haven for intentional destroyers of information, because a good faith requirement applies.

BUT

- It is unrealistic to expect parties to cease all routine information system operations as soon as they anticipate litigation may occur.
- The result would be even greater accumulation of duplicative and irrelevant data, increasing the cost and time burden of review and delaying proceedings.
- Once on notice of the need to preserve, the safe harbor only covers the gap between notice and reasonable ability to implement. Routine losses beyond that point are likely to speak to bad faith and spoliation, suggesting sanctions.

## Sanctions - Rule 37(f)

Routine Operations include:

- Recycling of back-up tapes.
- Recycling of operational material (video surveillance etc.).
- Automatic overwriting of deleted data.
- Automatic deletion of e-mail not accessed within pre-defined time period.
- Automatic updating of metadata through normal usage.
- Dynamic database information updated.

## Sanctions - Rule 37(f)

- A suspension of routine activities to preserve evidence is often termed a “litigation hold.”
- Rule 37(f) does not speak to litigation holds, but actions to implement such holds do suggest good faith.
- The scope of the litigation hold may be agreed by the parties during pre-trial discussions on data preservation mandated by amended Rule 26(f).
- If loss occurs in good faith, the revised rule permits sanctions only “in exceptional circumstances.”
  - Party seeking sanctions must show that the loss is highly prejudicial to its cause.
  - Even then, sanctions should only be to a level sufficient to remedy such prejudice.
  - Severe sanctions are generally to be restricted to situations where bad faith or reckless behavior is found.

## Proposed Fed. R. Evid. 502: Waiver of Privilege

- Rule 502 is the necessary counterpart to the civil procedure amendments on waiver of privilege.
- Inadvertent production of attorney/client or work product protected information not to constitute waiver if:
  - Disclosure was made in connection with federal litigation.
  - Respondent took reasonable precautions to prevent disclosure, and
  - Respondent took reasonably prompt measures on becoming aware of the disclosure to rectify the error.
- An agreement of the parties on the effect of disclosure on privilege will be binding on the parties to that agreement, and on other parties if it is reflected in a court order.

# Rule 502: A Caution

- No guarantee of final form, or date of federal applicability.
- Cannot bind state courts without statutory enactment by Congress. Unless this occurs, state courts may elect not to enforce waiver agreements.
- Can prudent counsel enter into agreements avoiding waiver when another court remains free to hold waiver occurred?
  - One court has stated that “[w]ithout such a definitive ruling no prudent party would agree to follow the procedures recommended.” *Hopson v. Mayor and City Council of Baltimore*, 232 F.R.D. 228, 234 (D. Md. 2005).
- Without Rule 502 will the civil procedure amendments succeed in reducing the cost and time burdens associated with handling the privilege issue in electronic discovery?

# Discovery Conferences Today

# Discovery Conferences Today

- Conferences must be in person: e-mail exchanges will not suffice. *Liebel-Flarsheim v. Medrad Inc.*, 2006 WL 335846 (S.D. Ohio).
- Respondents must be able to candidly discuss what they possess, and obstacles to search and retrieval.
- Requesting parties need to be able to articulate the objectives of discovery requests clearly. Courts may deny requests that do not enable potentially relevant information to be identified. See, e.g., *Wright v. AmSouth Bancorporation*, 306 F.3d 1198 (2<sup>nd</sup> Cir. 2003)

## Discovery Conferences Today

- Respondents must identify relevant accessible sources and state inaccessible ones by category and type to enable the requestor to evaluate the benefits and costs of discovery from such sources.
- Parties may request an opportunity to sample materials subject to burden testing under Rule 26(b) and (c). Courts will consider relative burdens and benefits of such a request.
- Discovery of inaccessible materials may be ordered for good cause.

## Discovery Conferences Today

- Requestor should identify the format in which electronic discovery is desired.
- Requestor should also explicitly identify any types of metadata sought.
- Both parties should identify key players and the individuals responsible for extracting pertinent information.
- Both parties should address preservation issues.
- Parties should discuss cost allocation.
- Parties should agree upon waiver of privilege and/or use of experts.

# Production Rules

## Production is required only once:

- A requesting party is only entitled to preferred form if it specifies that form. *Northern Crossarm v. Chemical Specialties* 2004 WL 635606 (W.D. Wis.) (a request for an electronic format, after production of 65,000 emails in paper form, was too late).
- Unless the original discovery request stipulates a specific electronic form, print-outs that mimic the form in which the data is electronically stored will satisfy discovery. *India Brewing, Inc. v. Miller Brewing Co.*, 2006 WL 2023396 (E.D. Wis.).
- Requestor should bear reasonable costs for reviewing duplicated data for privileged materials. *Dodge, Warren, & Peters Ins. Servs. v. Riley*, 130 Cal.Rptr.2d 385 (Cal. App. 2003).
- Duplicative discovery is inappropriate unless plaintiffs assume the cost. *Lipco Electrical Corp. v. ASG Consulting Corp.*, 2004 N.Y. Misc. LEXIS 1337 (N.Y. Sup. Ct.).

# Cost-Shifting Post Amendments

- Still generally applicable only to inaccessible data.
- Respondent must identify inaccessible sources, by type and category.
- Respondent need not search initially, but has burden of justifying inaccessibility.
- If shown, onus shifts to requesting party to show marginal utility of searching inaccessible sources.
- Rule 34(a)(1) enshrines sampling to allow better evaluation.
- *Rowe, Zubulake* and *Wiginton* type balancing tests endorsed.
- Rule 26(f) requirement that such issues be addressed in pre-trial conferences.

- Normal business form:
  - Disclosure responsive to requests, made in the form in which it was kept, satisfies the respondent's duty. *Eastman Kodak Co. v. Sony Corp.*, 2006 WL 2039968 (W.D. N.Y.)
  - Where documents are kept only in hard copy, the plaintiff is not entitled to any other format. *India Brewing, Inc. v. Miller Brewing Co.*, 2006 WL 2023396 (E.D. Wis.).
- Substitutes may not suffice:

Requestor has the right to choose between formats used in the normal course of business. Failure to disclose alternatives, or to provide the desired form, is a breach of duty even where the alternate is functionally equivalent. *In re Bristol Myers Squibb Sec. Litig.*, 205 F.R.D. 437 (D.N.J. 2002); *Milwaukee Police Assoc. v. Jones*, 615 N.W. 2d 190 (Wis. App. 2000).

- **Back-up Tapes:**

Although discovery from back-up tapes would be costly and time-consuming, the responding party had the burden of creating a retrieval system that would be less burdensome. An “otherwise good faith” discovery request could not be defeated in these circumstances. *Kaufman v. Kinko’s Inc.*, 2002 WL 32123851 (Del. Ch.).

- **Incompatible Data:**

Defendant is obligated to produce the information in a reasonably useable form. *Static Control Components, Inc. v. Lexmark Int’l, Inc.*, 2006 WL 897218 (E.D. Ky.) (Defendant not entitled to use the unique nature of a computer system to preclude relevant and comprehensible discovery).

# Protecting Privilege

# Waiver of Privileges in Electronic Discovery

- Approach 1: Lawyer cannot waive privilege
  - “The fact that such a document has been reviewed by counsel or by the expert shall not constitute a waiver of any claim of privilege or confidentiality.” *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421 (S.D.N.Y. Jan. 16, 2002).
  - Wisconsin has followed *Rowe*: “[A] lawyer, without the consent or knowledge of a client, cannot waive the attorney-client privilege by voluntarily producing privileged documents (which the attorney does not recognize as privileged).” *Harold Sampson Children’s Trust v. The Linda Gale Sample 1979 Trust*, 271 Wis. 2d 610 (Wis. 2004).

# Waiver of Privileges in Electronic Discovery

- Approach 2: Balancing Test - *Marrero Hernandez v. Esso Standard Oil Co.*, 2006 WL 1967364 (D. Puerto Rico):
  - Waiver determined by balancing test:
    - Reasonableness of precautions to prevent inadvertent disclosure.
    - Time it took the producing party to recognize error.
    - The scope of the production.
    - The extent of the inadvertent disclosure.
    - The overriding interest of fairness and justice.
  - The importance of the privilege demands great care. Lack of diligence left the defendant with nobody but itself to blame.

# Waiver of Privileges in Electronic Discovery

- Approach 3: Party Agreement - *Hopson v. Mayor and City Council of Baltimore*, 232 F.R.D. 228 (D. Md. 2005):
  - Parties encouraged to agree on a mechanism enabling allowing claw-back of materials disclosed.
    - Aimed at accelerated disclosure and reduction of front-end cost of screening for privilege.
  - Otherwise the court will determine a time scale and the extent of electronic discovery.
  - Waiver will not result from production of privileged or work product material inadvertently disclosed in response to such order.
- Accords with the rationale adopted in the new amendments to the Federal Rules of Civil Procedure.

# Problems with Privilege Agreements

Waiver Agreements have not always been honored:

- If, when, and in what form will proposed Fed R. Evid. 502 take effect, and will it bind state courts? Without it, there is no guarantee waiver agreements will be honored by other courts.
- Felt to lead to sloppy attorney review and improper disclosure which could jeopardize clients. *Koch Materials Co. v. Shore Slurry Seal Inc.*, 208 F.R.D. 109 (D. N.J. 2002).
- “Selective waiver” is not permitted: parties waiver agreement not enforced. *In re Quest Communications Intern. Inc.* 2006 WL 1668246 (10th Cir.).

## Other Means to Maintain Privilege – Independent Experts

- By mutual agreement, respondent selects a computer forensics specialist to conduct a relevancy review and make a “mirror image” of the respondent’s data source without waiver of privilege or other legal protections.
- Only employees of expert have access to equipment or data.
- Expert provides detailed report of what was inspected, extracted, and imaged to each party and the court.
- Respondent creates a privilege log, before production.
- If a dispute arises, the information will remain on an attorney’s-eyes-only basis until it is resolved.

## Other Means to Maintain Privilege – “Quick Peek”:

- By agreement or court directed.
- Often used when the requesting party has more resources than the responding party.
- Documents produced without review.
- Requestor identifies information it wants.
- Responding party then determines whether the requested materials are privileged.

## Caution – Direct Access By Other Parties

- Unfettered access undermines privacy. *Diepenhorst v. City of Battle Creek*, 2006 WL 1851243 (W.D. Mich.).
- A reasonable expectation of privacy exists. *In re John Doe Proceeding*, 272 Wis. 2d 208 (Wis. 2004).
- Less intrusive options exist: special master appointed to retrieve and identify any relevant information for court review). *In re Triton Energy Sec. Litig.*, 2002 WL 32114464 (E.D. Tex.).
- A request lacking adequate undertakings regarding the conduct of inspection risked harm to the data, system, privacy and privilege. *Fennell v. First Step Designs Ltd.*, 83 F.3d 526 (1st Cir. 1996).
- Absent a showing of non-compliance, such an inspection is merely a fishing expedition. *Bethea v. Civ. Action Comcast*, 2003 U.S. Dist. Lexis 21595 (D.D.C.).
- Direct Access is not justified to address the possibility of discovery misconduct. *Floeter v. City of Orlando*, 2006 WL 1000306 (M.D. Fla.).

# Ensuring Discovered Information is Admissible

## Caution: The Chain of Custody and Electronic Evidence

- Electronic information is easily altered, and hence is particularly suspect if a chain of custody cannot be established.
- This problem is commonly associated with respondents; however, any requesting party granted access to the systems of another, directly or via an expert, should take clear steps to establish and log procedures that will later support authentication.
- The mere possibility of tampering does not affect the authenticity of electronic information without some evidence that alteration occurred, *United States v. Whitaker*, 127 F.3d 595, 602 (7th Cir. 1997).
- Unrebutted allegations of alteration nevertheless undermine the weight of the evidence. *United States v. Bonallo*, 858 F.2d 1427, 1436 (9th Cir. 1988).

## The Chain of Custody and Electronic Evidence.

### *In re Vinhnee v. Vinhnee*, 336 B.R 437 (9th Cir. 2005)

- Electronic evidence is only admissible if “built-in safeguards to ensure accuracy and identify errors” are demonstrated.
- Requires testimony regarding policies relating to data collation, extraction, and system control procedures, including access privileges, logging of any changes, back-up practices and audit procedures.
- Adequate measures to ensure data integrity must be shown.
- Authentication requires a showing that the witness has sufficient training and experience to credibly assert integrity.
- In the absence of evidence of safeguards and acceptable authentication testimony by a plaintiff, there was no error in granting judgment for a defendant who did not even respond to the complaint.

# Conclusion

© Robert Gegios & Stephen Taylor, Kohner Mann & Kailas, S.C.