

Partner with:



### Digital Law Primer:

This is a recap of the key areas of law in which digital issues commonly arise. Some of these topics are undergoing rapid change – the purpose of this Primer is to focus you on what you should look for and bring current for your specific purposes. We can help you and your firm get up to speed quickly and efficiently. For starters, consider the current law on e-Data admissibility, a survey of recent e-Discovery cases that impose major sanctions and offer guidance in this area, and the pending and likely soon to be adopted e-Discovery amendments to the Federal Rules of Civil Procedure.

#### Admissibility of e-Evidence Is the Norm:

Courts have long recognized the validity of digital evidence as demonstrated by the now classical quote from *Harris v. Smith*, 372 F.2d 806 (8th Cir.1967):

...[N]o court could fail to notice the extent to which business today depends on computers for a myriad of functions. Perhaps the greatest utility of a computer ... is its ability to store large quantities of information which may be quickly retrieved on a selective basis. Assuming that properly functioning computer equipment is used, once the reliability and trustworthiness of the information put into the computer has been established, the computer printouts should be received as evidence of the transactions covered by the input.

The so-called Best Evidence Rule -- requiring an "original" document for admissibility -- was eroded by exceptions during the age of the copier, and is by now all but an historical footnote under modern laws reflecting the realities of the digital age.

See, for example: NRS 52.225, which includes "electronic" data as a form of writing for evidentiary purposes; the Nevada Uniform Electronic Transactions Act, NRS Chapter 719, which generally authorizes all records to be maintained and produced electronically; and the Federal Business Records Act, 28 USC 1732, which provides that even for governmental agency records, an image is as admissible as the original if the records are kept in the ordinary course of business in any medium that accurately reproduces the original. Nevada alone has hundreds of statutes

recognizing the validity and admissibility of digital media, including perhaps the most sacred bastion of "originals" -- Wills.

### **e-Discovery is Increasingly Mandatory – According To The Courts And Realities:**

Everyone is familiar with how Bill Gates' failure to recognize the potential impact of internal e-mails impaired his anti-trust defense. [His testimony was "I did not see that (acquiring Netscape) as something that made sense", but his e-mail said "We could even pay them (Netscape) money as part of the deal, buying a piece of them or something". Another e-mail from Mr. Gates to a Microsoft VP said "Do we have a clear plan on what we want Apple to do to undermine SUN."] One would think a major digital company such as Microsoft® would have anticipated and addressed such problems, but even it is still facing more problems with its e-mail policy.

A November 18, 2004 Associated Press article by Foster Klug entitled "[Microsoft Accused of E-Mail Scorched Earth Policy](#)" begins as follows: "Microsoft Corp. developed policies stressing the systematic destruction of internal e-mails and other documents crucial to lawsuits it has faced in recent years, a California software company alleges." [Read more](#) in the complete article as reprinted by Law.com®.

Obviously, e-mail policies along the extreme lines allegedly adopted by Microsoft® are not the solution. Without passing on the merits of either Microsoft's original policy of allowing anything to be put into internal e-mail form, or belatedly purging potentially harmful e-mails, a policy somewhere in the middle is obviously desirable to both prevent inclusion of inadvertently harmful evidence, and charges of willful destruction of potentially harmful materials.

But Microsoft® is not the only one to face such problems. More and more lawyers and clients are painfully finding out that proper e-Discovery retention policies and production are not optional. Digital shortcomings can result in major discovery sanctions, as well as the production of harmful data that never should have been created and perhaps should not have been produced, and/or the inability to analyze and segregate helpful data.

e-Discovery is also cost-effective. Keep in mind that Document discovery represents 50 percent of the litigation costs in the average case and up to 90 percent of the costs in an active discovery case. e-Discovery offers many advantages over traditional manual discovery methods:

- Reduced staff costs, which allows the case budget to be spent on analysis, not paper shuffling mechanics
- Increased computer accuracy over staff subject to human tolerances & errors
- Reduced time frames for computerized organization & reviews
- Ability to immediately re-analyze e-Data as case focus develops & shifts

See our Conclusion below for suggestions on how to properly designed Enterprise Content Management (ECM ) digital storage and retrieval systems and protocols can help reduce discovery costs, avoid the Microsoft®-type problems and facilitate compliance with the new Federal e-Discovery Rules as well as regulatory requirements.

### **Survey of Recent e-Discovery Cases:**

Many of the evolving e-Discovery cases concern the failure to preserve e-Data – typically e-mail – during the litigation and who should bear the cost of producing e-Data that is not readily "accessible" (e.g., has been deleted or is storage in a format that requires special forensic recovery procedures).

In some cases, the focus has shifted from the merits to the e-Discovery failures with severe monetary sanctions to accomplish the e-Discovery, exclusion of non-compliant key witnesses, and what has been referred to as the "death sentence" of adverse inference, or even default judgment. e-Discovery failures can turn a marginal case into a winner.

The current waive of e-Discovery holdings are an extension of traditional standards that have recognized even "inaccessible" e-Data as being discoverable, and application of the discovery burden shifting standards to e-Data that has been deleted or stored in a format that is not readily "accessible".

A few slightly older cases, a reference to FRCP 26, and the old maxim *omnia presumuntur contra spoliatores*: "all things are presumed against a despoiler or wrongdoer" [Black's Law Dictionary at p. 1086 (6<sup>th</sup> Ed. 1997)] should provide the background transition.

*Simon Property Group, LP v My Simon, Inc.*, 194 FRD 639, 640 (SD Ind. 2000) held that "computer records, including records that have been 'deleted' are documents discoverable under FRCP 34." See also, *Antioch Co. v Scrapbook Borders, Inc.*, 210 FRD 645 (D. Minn 2002), which ordered preservation and forensic recovery of deleted e-mails under a specified protocol.

Under FRCP 26, the general presumption is that the producing party must bear the cost of production, subject to the court's discretion under FRCP 26(c) to protect a party from "undue burden or expense" by shifting the production costs to the requesting party.

*Rowe Entertainment, Inc. v The William Morris Agency*, 205 FRD 421 (SDNY 2002) adopted a generally accepted balancing approach based on eight factors to determine whether discovery costs should be shifted from the producing party to the requesting party:

- Specificity of the request
- Likelihood of discovering critical information
- Availability of the information from other sources
- Purpose for which the responding party maintains the data
- Relevant benefits to the parties from the data
- Total cost of the production
- Relative ability of each party to control costs and its incentive to do so
- Resources available to each party

*US v. Phillip Morris, USA, Inc.*, 321 F. Supp. 2d 21 (DDC 2004) (Case No. 99-2496) made it painfully clear to the tobacco company that e-mails should not be deleted during litigation. After the court's initial discovery order requiring preservation of all potentially relevant documents, the defendant began deleting e-mails over 60 days old. The court imposed the following sanctions: No employee who participated in the deletions (which included a number of top executives) could testify at trial; an expert was excluded; and \$2.75 million of monetary sanctions (based upon the estimated cost of the requesting party to forensically recover the deleted e-Data).

*Mosaid Techs., Inc. v Samsung Elecs. Co.*, No. 01-VC-4340 (D.NJ July 7 2004) and Sept. 1, 2004) rejected Samsung's argument that deletion of e-mails was not violative of a discovery request that did not specifically mention e-mails, and imposed a \$566, 838 sanction for recovery costs and an adverse inference instruction for the e-mail spoliation.

*Anderson v Crossroads Capital Partners, LLC*, 2004 WL 256512 (D. Minn, Feb. 10, 2004) issued an adverse jury instruction based on willful destruction of previously deleted computer files to suppress the truth after forensic expert testified that a data wiping software application had been installed after the court had ordered preservation.

In *Kucala Enterprises v Auto Wax*, No 02C1403, 2003 Lexis 8833 (ND II. May 23, 2003), the Magistrate recommended dismissal with prejudice after plaintiff installed and used a data wiping software on two computers and throwing away another computer before defendant's expert could conduct the court ordered forensic inspection. The district court adopted the Magistrate's findings but reduced the dismissal sanction in *Kucala* 2003 Lexis 19103, 57 Fed. R. Serv. 3d (ND II. Oct. 27, 2003), and later in *Kucala* 2004 Lexis 5723 (ND II. April 6, 2004) awarded monetary sanctions of \$93,125.74.

But it can get worse for the unwary lawyer and client. *Procter & Gamble Co. v Haugen*, 2003 WL 2280734 (D. UT Aug. 19, 2003) resulted in entry of a defense judgment after plaintiff Procter & Gamble willfully deleted electronic financial information in the so-called Satanic Message case: "the Court is convinced that Plaintiffs have failed to preserve relevant electronic data that Plaintiffs knew was critical to their case and to the defense."

And much worse yet – *Coleman (Parent) Holdings, Inc. v Morgan Stanley & Co., Inc.*, 2005 WL 679071 (Fla. Cir. Court March 1, 2005) involved alleged misrepresentation of the value of an investment, but ended focusing on Morgan Stanley's failure to produce e-mails. The court found this failure to be so willful that it shifted the burden to Morgan Stanley to prove it did not defraud the investor: "5. MS & Co. shall bear the burden of proving to the jury, by the greater weight of the evidence, that it lacked knowledge of the Sunbeam fraud and did not aid and abet or conspire with Sunbeam to defraud [CPH]. The traditional order of proof shall remain unaffected, however."

The resulting \$1.4 billion (not million) judgment against Morgan Stanley shows it could not stasis this burden. A March 23, 2005 Wall Street Journal article quoted Morgan Stanley as saying they had fired, and were considering a malpractice action against, the lawyers who had handled the case up to that point, and had represented Morgan Stanley for years. Preliminary comments indicate the basis for this client effort to shift liability to its lawyers will be that the lawyers did not adequately advise the client as to the potential risks of its discovery failures.

Another devastating result from e-Discovery gamesmanship has just been unsealed in two Ohio cases by Texlon against Price Waterhouse Coopers LLP (US District Case Nos. 5:98CV2876 & 1:01CV 1078): "Because PwC's conduct has made it impossible to try this case with any confidence in the justice of the outcome, PwC should bear the burden created by its conduct. For this reason, the magistrate judge recommends that the court grant Texlon's and plaintiffs' motions and enter default judgments against PwC and in favor of Texlon and plaintiffs in [these] cases." This would amount to a \$345 million fine for stalling and mishandling the production of documents.

Surveys by Bowne/DecisionQuest in 2003 show that juror's are ripe to grant large awards against those who face e-Discovery adverse presumptions: 78% agree that companies destroy documents hoping to avoid responsibility for their actions; 85% agree that large companies tend to hide adverse information.

Other surveys show client managerial awareness of, but the failure to address, these problems: 93% admit e-Data management procedures will be important in future litigation, but only 41% of companies have a e-mail retention policy and 46% do not have any litigation hold procedure in place.

A motion to preserve e-Data can give the moving party additional protections from inadvertent loss, and a strong ground from which to later complain about any actual lost e-Data. *Capricorn Power Co., Inc. v Siemens Westinghouse Power Corp.*, Civ. 01-39J, 2004 WL 870659 (WD Pa

April 21, 2004) applied a three factor balancing test to determine whether to preserve e-Data (an expensive and disruptive burden on the preserving party): Level of court's concern for continuing existence of the integrity of the e-Data, likelihood of irreparable harm to party seeking preservation absent compelled preservation, and capabilities to and burdens upon the persevering party from preservation.

Even without a protective order, each party has a duty to competently search and produce his e-Data. *Gates Rubber Co. v Bando Chem. Indus., Ltd*, 167 FRD 90 (DC Colo 1996) held that when processing e-Data, the party has the "duty to utilize the method which would yield the most complete and accurate results".

Cost sharing motions can shift the producing party's burden in some cases. *Wiginton v Ellis*, 2004 WL 1895122 (ND II. 2004) focused on the importance of requested discovery in resolving the litigation issues, including the availability of other evidence, in shifting ¾ of the cost of analyzing 94 e-mail back up tapes to the requesting plaintiff-employees who alleged the tapes would contain pornographic e-mails that created a hostile work environment.

*Ports v City of Chicago*, 2004 WL1535854 (ND II July 7, 2004) required the requesting City to pay half of the cost to compile requested e-Database.

The format of the e-Data produced must meet useable standards. *In re Verisign, Inc. Sec. Litig.*, 2004 WL 2445234 (ND Cal. Mar. 10, 2004) rejected a TIFF format production and required e-mails to be produced in their "native" .pst format as stored in the ordinary course of business. Accord, *Zakre v Norddeutsche Landesbank Girozentrale*, 2004 US D. Lexis (SDNY Feb. 11, 2004) (format should be "searchable" or as documents were kept in the "usual course of business")

While most of the decisions have involved e-mails, courts are starting to consider voicemail (VM) messages and instant messages (IM's). *In Burrell v Anderson*, 353 F. Supp. 2<sup>nd</sup> 55 (D Me 2005), the court held that defendant's had no obligation to retain one-sided voicemail messages that might have been favorable to plaintiff.

But in *Icu Med., Inc. v B. Braun Med., Inc.*, 2005 WL 1511927 (ND Cal. Jan. 4, 2005) the plaintiff was compelled to search "all computerized files, emails, voicemails, work files, desk files, calendars and diaries, and any other locations and sources if materials of the type to be produced might plausibly be expected to be found there".

In *Convolve, Inc. v Compaq Computer Corp.*, 223 FRD 162 (SDNY 2004), the court in footnote 4 recognized the "somewhat analogous situation ... in the use of Instant Messenger functions", but left open "the circumstances under which the failure to preserve Instant Message communications would be considered spoliation."

*State v Voorheis*, 2004 WL 258178 (Vt. 2004) held that IM's were sufficient to support a criminal conviction.

The most publicized and widely considered line of e-Discovery decisions have been issued in *Zubulake v UBS Warburg LLC*, (SDNY, Case No. 2 Civ 1243), a wrongful termination case (gender discrimination and illegal retaliation) that was effectively determined in discovery. Some of defendant's employees disregarded a discovery order to preserve evidence and deleted e-mails that plaintiff contended were crucial and available in backup tapes.

The defense's e-Data stonewalling blew up in its face when it came out that plaintiff had taken hundreds of e-mails with her when she left, yet none were produced. The court focused on one particularly abusive deleted e-mail that the plaintiff had which included the following harmful statement: "She's old, ugly and can't do the job."

In a series of five decisions, the trial court developed a pretty good body of e-Discovery law in its own right, and for sanctions (i) required the defendant to pay the fees and costs of re-deposing those employees involved, and (ii) imposed jury instructions permitting assumption of adverse inferences from the missing items. The sixth decision showed the real cost of these violations – a \$9.1 million compensatory award and a \$20.1 punitive damages award.

Here's a recap of the e-Discovery rules developed in the *Zubulake* decisions:

- *Burden shifting* – based on the state of the existing e-data; if that data is accessible, then there is no burden shifting (a tightening of prior burden shifting cases); if inaccessible, then apply burden shifting factors (a modified *Rowe* standard), which include relevancy of request, availability from other sources, cost of production in relation to amount in controversy and resources of both parties, relative abilities and incentives to control costs, importance of relevant issues, and relative benefits to requesting information
- *Key players* – those e-Data custodians likely to have relevant information automatically have the duty to preserve
- *Obligations to preserve* – a party must suspend its routine retention-destruction policies and put a litigation hold in place to ensure preservation once litigation is reasonably anticipated; but does not apply to inaccessible back up tapes which can be recycled under the standard policy (though there are contrary decisions requiring back up tapes to be held)
- *Sanctions for spoliation* – burden of proof to receive adverse inference instruction is that opposing party destroyed evidence that would have been favorable; prove a negative by willfulness as evidence of the relevance; spoliation instruction permits, but does not require, the jury to infer that destroyed evidence material to the facts would have been unfavorable
- *Duties for counsel* – must promptly issue a litigation hold, communicate directly with key players & instruct production of all e-copies of relevant documents; active supervision & sampling are required – must know the client's e-Data system, work with IT staff, run & preserve searches to ensure compliance

### **e-Discovery Amendments To The Federal Rules Of Civil Procedure**

The number of e-Discovery cases is rapidly growing, and the Federal Judiciary's Advisory Committee on Civil rules has published and received comments on its proposed changes to the FRCivP. These proposals use multiple-tiers and a safe-harbor rule, and undoubtedly represent the trend for all e-Discovery.

*Here is a recap of the proposed Rule changes affecting digital discovery:*

Rule 16 – (Pretrial Conferences; Scheduling; Management) (establishes process for the parties and court to address early issues pertaining to the disclosure and discovery of electronic information)

Rule 26 – (General Provisions Governing Discovery; Duty of Disclosure) (requires parties to discuss during the discovery-planning conference issues relating to the disclosure and discovery of electronically stored information)

Rule 33 -- (Interrogatories to Parties) (expressly provides that an answer to an interrogatory involving review of business records should involve a search of electronically stored information)

Rule 34 -- (Production of Documents and Things and Entry Upon Land for Inspection and Other Purposes) (distinguishes between electronically stored information and "documents")

Rule 37 -- (Failure to Make Disclosure or Cooperate in Discovery; Sanctions) (creates a "safe harbor" that protects a party from sanctions for failing to provide electronically stored information lost because of the routine operation of the party's computer system)

Rule 45 -- (Subpoena) (technical amendments that conform to other proposed amendments regarding discovery of electronically stored information)

Rule 50 -- (Judgment as a Matter of Law in Jury Trials; Alternative Motion for New Trial; Conditional Rulings) (permits renewal after trial of any Rule 50(a) motion, deleting the requirement that a motion made before the close of all the evidence be renewed at the close of all the evidence)

Form 35 -- (Report of Parties' Planning Meeting) (technical revision reflecting the proposed amendment to Civil Rule 26)

Go to: [uscourts.gov/rules](http://uscourts.gov/rules) for more details, the comments submitted and the current status of the proposed changes.

### **Conclusion:**

Properly designed ECM digital storage and retrieval systems and protocols can dramatically reduce discovery costs and help avoid such e-Discovery disasters for your clients or your business, and can put a digitally-impaired opponent at a serious disadvantage in both dealing with your digital production and making his production to you. We can help law firms and clients deal with these problems preferably before, but also during, litigation.

An ECM overhaul *in advance of* litigation will be both less costly and more effective by preventing the ill-advised document generation, retention and destruction practices of your client or your business *before* they become the subject of discovery orders. This can, and should, include a regulatory compliance system as part of the comprehensive ECM design. Once litigation is pending, proper use of digital techniques can still minimize the adverse evidentiary results and sanctions that might otherwise result.