

# Electronic Discovery - New Amendments to the Federal Rules of Civil Procedure

Presented by:

David G. Concannon , Esquire  
Law Offices of David G. Concannon , LLC  
200 Eagle Road, Suite 116  
Wayne, Pennsylvania 19087  
Phone: (610) 293 8084  
Fax: (610) 293 8086  
concannonlaw@msn.com  
[www.davidconcannon.com](http://www.davidconcannon.com)

**DAVID G. CONCANNON** is the principal in the Law Offices of David G. Concannon, LLC in Wayne, Pennsylvania. He practices in the areas of commercial litigation, intellectual property, sports and recreation law, product liability and trade secret litigation in state and federal courts nationwide.

Mr. Concannon has been recognized as a “Super Lawyer” in Business Litigation in the 2006 and 2007 editions of *Pennsylvania Super Lawyers*. In 2005, Concannon was recognized as a “Rising Star” in the area of Business Litigation. Since establishing his law firm in 2002, Mr. Concannon has achieved more than \$38 million in settlements and verdicts on behalf of the firm’s business clients, while he has also successfully defended more than \$100 million in claims asserted against the firm’s clients. Mr. Concannon achieved one of the top 50 jury verdicts in the United States in 2005, in a case that also achieved the second highest jury verdict in Pennsylvania and one of the highest jury verdicts ever recorded in a tortious interference case.

Mr. Concannon is a December 1990 graduate of the Widener University School of Law in Wilmington, Delaware. Prior to graduation, he studied international law in Africa and Europe. After working for Conrad, O’Brien, Gellman & Rohn in Philadelphia for one year, Mr. Concannon served as a law clerk to the Honorable Louis C. Bechtle, Chief Judge of the United States District Court for the Eastern District of Pennsylvania, from 1992 to 1995. Before founding his own law firm, he was associated with Kohn, Swift & Graf, P.C. in Philadelphia.

Mr. Concannon is admitted to the State Bars of Pennsylvania and New Jersey; the United States Supreme Court; the United States Courts of Appeals for the First, Third, Fourth and Ninth Circuits; and the United States District Courts for the Eastern District of Pennsylvania, Middle District of Pennsylvania and the District of New Jersey. He has been admitted pro hac vice in state and federal courts in California, Florida, Illinois, New Hampshire, Rhode Island and Maine.

# Electronic Discovery - New Amendments to the Federal Rules of Civil Procedure

On December 1, 2006, the Federal Rules of Civil Procedure were amended in several key areas to address the realities of electronic discovery. The amendments were also adopted by several states, including New Jersey. The new amendments address five related areas:

- (1) early attention to issues relating to electronic discovery, including the form of production, preservation of electronically stored information, and review of electronically stored information for privilege;
  - (2) discovery of electronically stored information that is not reasonably accessible;
  - (3) the assertion of privilege after production;
  - (4) the application of Rules 33 and 34 to electronically stored information; and
  - (5) a limit on sanctions under Rule 37 for the loss of electronically stored information as a result of the routine operation of computer systems.
- 
- In addition, amendments to Rule 45 are made to correspond to the proposed changes in Rules 26-37.

# Early Attention to Issues Relating to Electronic Discovery

Ignorance is no longer an excuse. Attorneys are now expected to live in the digital age.

The amendments to Rule 16 (Pretrial Conferences; Scheduling; Management) and Rule 26 (General Provisions Governing Discovery; Duty of Disclosure) set up a framework for the parties and court to give early attention to issues pertaining to the disclosure and discovery of electronic information.

Under the amendments to Rule 26(f), the parties must discuss during the discovery-planning conference any issues relating to the disclosure and discovery of electronically stored information, including the form of production, and also discuss issues relating to the preservation of electronically stored information and other information. The amendment also calls for discussion of whether the parties can agree to production on terms that protect against privilege waiver.

Form 35 (Report of Parties' Planning Meeting) is amended to reflect the Rule 26(f) changes.

Under amended Rule 16, the scheduling order may include provisions on the disclosure or discovery of electronically stored information and may adopt the parties' agreements for protection against waiving privilege.

Under the amendments to Rule 26(b)(2)(C), a party need not provide electronically stored information in response to a discovery request if the information is not reasonably accessible.

The term "not reasonably accessible" is undefined. Instead, whether information is "not reasonably accessible" will be decided on a case-by-case basis. (Expect lots of litigation on this issue, and lots of overworked federal magistrates.)

If the requesting party moves to compel discovery of such information, the responding party must demonstrate that the information is not reasonably accessible. If that showing is made, the court may still order the party to provide the information, if the requesting party shows good cause. After good cause is shown, the court may – as with any discovery – impose conditions and terms on the discovery of electronically stored information that is not reasonably accessible.

# Inadvertent Production and Waiver of Privilege

Amended Rule 26(b)(5)(B) sets up a procedure for a party to assert that it has produced privileged information without intending to waive the privilege (i.e., the “Claw Back Procedure”).

The amended rule allows the party who has responded to a discovery request to notify the receiving party that it is asserting a privilege within a reasonable time after production.

After receiving notification, the receiving party must return, sequester, or destroy the information, and may not disclose it to third parties.

The producing party must preserve the information and put it on a privilege log, pending the court’s ruling, on a motion to compel, whether the information is, in fact, privileged and whether any privilege has been waived or forfeited by production.

The amended rule does not address whether there has been a privilege waiver.

# Discovery Requests

The amendments to Rule 33 (Interrogatories to Parties) and Rule 34 (Production of Documents and Things and Entry Upon Land for Inspection and Other Purposes) clarify their application to electronically stored information and provide a framework for resolving disputes.

The Rule 33 amendments make it explicit that an answer to an interrogatory involving review of business records should involve a search of electronically stored information and permit the responding party to answer by providing access to that information.

The Rule 34 amendments distinguish between electronically stored information and “documents,” expansively defining each to avoid limitation to existing technologies.

The amendments to Rule 45 (Subpoena) are technical in nature and conform to changes in other discovery rules relating to discovery of electronically stored information.

# Form of Production

The amendments to Rule 34(b) also permit the requesting party to specify the form in which electronically stored information is to be produced and permit the responding party to object to the requested form.

If there is no request for a specific form for producing electronically stored information, and if the parties do not agree to a particular form and the court does not order one, the producing party has two options: (1) to produce the information in a form in which it is ordinarily maintained, or (2) in an electronically searchable form.

Absent court order or party agreement, the responding party need only produce the information in one form.

# Sanctions

Amended Rule 37 (Failure to Make Disclosure or Cooperate in Discovery; Sanctions) adds a new subdivision (f) 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.

This limited “safe harbor” is not available if the party violated an order issued in the action requiring it to preserve electronically stored information, or if the party failed to take reasonable steps to preserve the information after it knew or should have known the information was discoverable in the action.

This new section addresses a unique and necessary feature of computer systems – the automatic recycling, overwriting, and alteration of electronically stored information.

The Advisory Committee is continuing to examine the degree of culpability or fault that will defeat safe harbor protection in this narrow area, but the federal courts are not waiting for an answer.

# Recent Case law

## Document Retention Policy

Defendant's Document Retention Policy "Clearly Relevant" and Must Be Produced

*Petersen v. Union Pacific R.R. Co.*, 2006 WL 2054365 (C.D. Ill. July 21, 2006).

In this opinion, the magistrate judge overruled defendant's objections to certain discovery requests, reminding the parties: "Remember, we are talking discovery, not admissibility at trial." One of the disputed requests for production sought defendant's document retention policy.

# Sanctions

Court Awards \$45,162 in Fees and Costs for Sanctions Motion, to be Shared Equally by Defendants and Their Counsel

*Phoenix Four, Inc. v. Strategic Res. Corp.*, 2006 WL 2135798 (S.D.N.Y. Aug. 1, 2006).

Plaintiff sought \$60,216 in fees and costs, and the defendants argued that plaintiff was to a maximum amount of only \$17,658.

The court reduced the requested total by 25 percent, finding that (1) some of the time incurred by plaintiff's counsel in reviewing documents would have been incurred anyway; and (2) the firm's use of block billing made it impossible to identify the work specifically related to the motion, and separate it from unrelated work. Accordingly, the court granted plaintiff's request for attorney's fees and costs associated with bringing the motion for sanctions in the sum of \$45,161.82, to be paid equally by the defendants and their law firm.

## More Sanctions

WTC Insurer and Its Counsel Hit with \$1.25 million E-Discovery Sanctions

*In re Sept. 11th Liab. Ins. Coverage Cases*, 2007 WL 1739666 (S.D.N.Y., June 18, 2007)

The perils of e-discovery were highlighted in the insurance coverage battles resulting from the September 11, 2001 terrorist attack on the World Trade Center. On June 18, 2007, the United States District Court for the Southern District of New York, sanctioned Zurich American Insurance Company (“Zurich”) and its counsel, the law firms of Wiley Rein LLP and Coughlin Duffy LLP, \$1.25 million upon finding that Zurich: (a) asserted unsupported defenses, (b) deleted electronic evidence, and (c) delayed the production of a 62-page insurance policy and other relevant documents.

At the heart of this insurance coverage action is the question whether the Port Authority of New York and New Jersey (“Port Authority”) and Westfield Corporation, Inc. (“Westfield”) are named insureds under a general liability policy issued to World Trade Center Properties LLP (“WTCP”). Zurich alleged that they were not. Zurich ultimately changed its position, however, when it produced documents that proved otherwise, long after those documents were first requested. These critical documents were in Zurich’s counsel’s possession for almost three years before they were produced. Concerned about the appearance of pleading and discovery abuses, the Court permitted the Port Authority and Westfield to seek sanctions under Rules 11 and 37 of the Federal Rules of Civil Procedure.

# Cost Recovery

Court Awards Prevailing Party \$4.6 Million in Costs for Litigation Database Creation

*Lockheed Martin Idaho Techs. Co. v. Lockheed Martin Advanced Envtl. Sys., Inc.*, 2006 WL 2095876 (D. Idaho July 27, 2006).

In this diversity case, the federal district court awarded the prevailing party its costs under 28 U.S.C. § 1920(4) in three areas: (1) \$4.6 million in costs for creating a litigation database; (2) \$600,000 in costs for trial evidence presentation; and (3) \$200,000 in costs for copies.

# Spoliation of Evidence

Spoliation Inference Further Supports Court's Finding that Defendant Infringed Motion Picture Copyrights

*Paramount Pictures Corp. v. Davis*, 2006 WL 2092581 (E.D. Pa. July 26, 2006).

In an earlier opinion (*Paramount Pictures Corp. v. Davis*, 234 F.R.D. 102 (E.D. Pa. 2005), the court denied summary judgment but concluded that an adverse inference sanction was warranted based upon defendant's spoliation of evidence.

The court awarded \$50,000 in statutory damages under 17 U.S.C. § 504(c) and entered a permanent injunction that enjoined defendant "from directly or indirectly infringing plaintiff, Paramount Picture Corp.'s, rights in the motion picture 'Lemony Snicket's: A Series of Unfortunate Events'."

# Safe Harbor Provision

Rule 37(f) Safe Harbor Provision Requires a Routine System in Place and Some Affirmative Action by Party to Prevent System from Destroying or Altering Information

*Doe v. Norwalk Community College*, 2007 WL 2066497 (D. Conn. July 16, 2007).

In reaching its decision, the Court noted that the Commentary to Rule 37(f) indicates that, “[w]hen a party is under a duty to preserve information because of pending or reasonably anticipated litigation, intervention in the routine operation of an information system is one aspect of what is often called a ‘litigation hold.’ Thus, to take advantage of the good faith exception, a party needs to act affirmatively to prevent the system from destroying or altering information, even if such destruction would occur in the regular course of business. “Because the defendants failed to suspend it at any time . . . the court finds that the defendants cannot take advantage of Rule 37(f)'s good faith exception.”

# Form and Scope of Production

Court Defers Ruling on Whether Additional E-mail Searches Are Necessary, Ordering Producing Party to Submit Detailed Affidavit re: Scope of Search

*Peskoff v. Faber*, 2006 WL 1933483 (D.D.C. July 11, 2006).

Court Denies Motion to Compel Plaintiff to Correlate Information Produced Electronically to Particular Document Requests

*Eastman Kodak Co. v. Sony Corp.*, 2006 WL 2039968 (W.D.N.Y. July 20, 2006).

Court Quashes Subpoena to Defendants' Computer Forensics Consultant

*Trammell v. Anderson Coll.*, 2006 WL 1997425 (D.S.C. July 17, 2006).

Just when you thought judges were unsophisticated...

Court Selects Search Terms and Sets Out Detailed Electronic Discovery Protocol in Light of Parties' Inability to Collaborate

*Williams v. Taser Int'l, Inc.*, 2007 WL 1630875 (N.D. Ga. June 4, 2007).

The court in this wrongful death case had previously held a hearing on outstanding discovery issues, and had directed each party to submit a proposed protocol to govern electronic discovery in the case. Based on the parties' filings, their representations during the hearing, as well as their submissions of electronic discovery protocols, the court entered this order resolving a variety of discovery disputes.

On the subject of electronic discovery, the court noted that a number of issues had arisen with respect to Taser's search of electronic databases of internal communications. In particular, the parties substantially disagreed about the manner in which the searches for responsive documents contained within these databases were to be performed. The disagreement focused in large part on the timing of that production, the specific search terms to be used, and the extent to which plaintiffs would be allowed to participate in the search process.

# Waiver of Privilege

Ex-Employee Waived Attorney-Client Privilege as to Deleted E-mails Later Recovered from Employer-Provided Laptops

*Kaufman v. SunGard Inv. Sys.*, 2006 WL 1307882 (D.N.J. May 10, 2006) (Unpublished).

BUT

District Court Affirms Magistrate's Decision Finding No Privilege Waiver as to Personal Files Stored on (but Later Deleted from) Employer-Provided Laptop

*Curto v. Med. World Communications, Inc.*, 2006 WL 1318387 (E.D.N.Y. May 15, 2006).

In this opinion, the district court denied defendants' objections to a magistrate's discovery order which concluded that plaintiff had not waived any attorney-client privilege or work product protection as to documents originally created on (but subsequently deleted from) two employer-provided laptops.

## Last But Not Least...

Court's Chambers Used to Make Forensic Image of Defendant's Hard Drive

*Warner Bros. Records, Inc. v. Souther*, 2006 WL 1549689 (W.D.N.C. June 1, 2006).

Plaintiffs sued for copyright infringement, contending defendant unlawfully downloaded and distributed copyrighted materials through the use of a peer-to-peer, online media distribution system. Defendant denied the allegations and also denied giving anyone permission to use the computer to conduct the activities complained of. Discovery disputes ensued.

The court ordered defendant's counsel to bring the computer to a hearing so it could determine whether to allow the plaintiffs to examine the computer. Plaintiffs' counsel assured the court his forensic technician, who was present in court, could copy the computer's electronic contents without injuring the computer. The court ordered that the computer be taken into the court's chambers so the forensic technician could make a copy of the computer's electronic information while further proceedings were taking place in the courtroom. The document and file retrieval was accomplished forthwith.

# Admissibility of Electronic Evidence

The admissibility of electronic data into evidence carries the same burdens as data stored on paper or witness testimony. However, just because it is easy to store and retrieve data kept in electronic form, that does not make it any easier to have this information admitted as evidence at trial. Because electronic evidence is so easy to manipulate, the standards for authentication are often heightened.

For example, say you plan to prove damages with your client's electronic database that tracks the outstanding account due. You will overcome the hearsay rule because the data is a business record; the account data was entered by persons with knowledge as a regular practice in the ordinary course of business. But with electronic documents there is an extra step. In *Vee Vinhnee v. American Express*, 336 B.R. 437 (9th Cir. 2005), the court pointed out that authenticating a paperless electronic record in principle poses the same issue as for a paper record. But because "one must demonstrate that the record that has been retrieved from the file, be it paper or electronic, is the same as the record that was originally placed into the file," there is an important distinction.

When one retrieves the paper that was put in the file, there usually is no issue that it may have been altered after its creation. But when one retrieves an electronic file, there must be some showing that the computer system ensures the integrity of the original because "digital technology makes it easier to alter the text of documents that have been scanned into a database, thereby increasing the importance of audit procedures designed to ensure the continuing integrity of the records." *Id.* at 445.

# The Bible on the Admissibility of Electronic Evidence

In May 2007, Maryland Chief Magistrate Judge Paul Grimm produced an extensive, thorough tutorial on the admissibility of electronic evidence in *Lorraine v. Markle American Insurance Co.*, 2007 U.S. Dist. Lexis 33020 (D. Md. 2007).

In *Lorraine*, the parties had filed cross-motions for summary judgment in a dispute involving \$36,000. Both motions were supported with hard copies of e-mails. It does not appear that either party objected to the other's use of the e-mail, but Judge Grimm did. Because Rule 56 of the Federal Rules of Civil Procedure requires that summary judgment motions be supported with admissible evidence, Judge Grimm felt constrained to inquire on his own whether the proffered e-mails were in fact admissible.

Concluding that they were not, he denied both motions without prejudice, and while the parties scrambled to settle their case before fees exceeded the amount at issue, Judge Grimm used the opportunity to issue a 101-page opinion that exhaustively sets out the admissibility problems of electronic evidence.

If you read just one decision regarding the admissibility of electronic evidence, read *Lorraine*.

# WHAT A DIFFERENCE A DECADE MAKES

## THE “VOODOO” INTERNET AND “UNTRUSTWORTHY” DATA

In *St. Clair v. Johnny's Oyster & Shrimp Inc.*, 706 F. Supp. 2d 773 (S.D. Texas 1999), the issue was who owned the ship on which the plaintiff was injured. The plaintiff sought to prove that by offering information taken from the U.S. Coast Guard Vessel Database Web site, the Coast Guard's official Web site and a government record, right?

No, not even close. Finding the electronic evidence totally insufficient, U.S. District Judge Samuel Kent observed that anything found on the Internet is “voodoo information” and “inherently untrustworthy” because “hackers can adulterate the content on any Web site from any location at any time.”

Fortunately, times have changed, and Judge Kent recently revisited his “Voodoo” Internet finding.

In *Diamond Offshore Servs. Co. v. Gulfmark Offshore Inc.*, 2007 U.S. Dist. Lexis 5483 (S.D. Texas 2007), Kent acknowledged that companies are increasingly utilizing the Internet, but he reiterated that he still finds Internet evidence inherently untrustworthy.

The fact is, electronic evidence is not automatically deemed to be reliable, trustworthy and easily admissible. Electronic evidence brings unique baggage to the admissibility equation that we need to think through very carefully.

# E-Mail

E-mail is often the most explosive form of electronic evidence. However, e-mail carries its own problems when it comes to admissibility.

For an e-mail to be admissible, you will need to show, among other things, that it is authentic and it is not hearsay. E-mail chains present particular problems, because they are often a combination of party admissions, business records, nonparty hearsay and self-serving statements. So even if the admissibility of part of an e-mail chain is clear, you may need to look at each and every link. See, e.g., *Rambus Inc. v. Infineon Technologies A.G.*, 348 F. Supp. 2d 698 (E.D. Va. 2004).

Don't expect the court to assume that an e-mail is authentic simply because it is gleaned during discovery. In *U.S. v. Safavian*, 435 F. Supp. 2d 36 (D.D.C. 2006), the court took a lenient view on authenticity and decided that the possibility that e-mails might have been altered does not in itself justify their exclusion, since any form of documentary evidence can be altered. But it takes some skill to forge a paper signature; altering an e-mail takes nothing more than an impure heart and a keystroke.

And as Judge Grimm pointed out in *Lorraine*, because “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 ... 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.”

Despite the problems with its admissibility, e-mail is often worth the trouble. In fact, it's often worth its weight in gold.