

Avoiding The Pitfalls Of Electronic Discovery

by
Matthew M. Neumeier, Esq.
and
Brian D. Hansen, Esq.

Jenner & Block, LLC
Chicago

**A commentary article
reprinted from the
November 2003 issue of
Mealey's Litigation Report:
Discovery**

JENNER & BLOCK
Bits and Bytes of Electronic Discovery***Avoiding The Pitfalls Of Electronic Discovery***

By
Matthew M. Neumeier
and
Brian D. Hansen

[Editor's Note: This is the first in a series entitled "Bits and Bytes of Electronic Discovery." Matthew M. Neumeier is a partner at Jenner & Block, LLC in Chicago and Co-Chair of the firm's Class Action Litigation and Products Liability and Mass Tort Defense practice groups. Mr. Neumeier speaks and writes frequently on the topic of electronic discovery, and teaches an L.L.M. course on High Technology Litigation at The John Marshall School of Law. Brian D. Hansen is an associate at Jenner & Block, LLC and a member of the firm's class action and litigation practice groups. The authors would like to thank Kelly A. James for her research and assistance with this article. Replies to this column are welcome. Copyright 2003 by the authors.]

Introduction

The digital revolution has changed the face of litigation. Numerous corporations are transitioning to a "paperless environment." It has been estimated that over 93% of all information generated today is in electronic form.¹ The benefits of the electronic revolution to businesses are great. Electronic data is more easily organized, accessed, manipulated and stored than its paper counterpart. The digital revolution, however, also has exponentially increased the volume of information within a company's possession, custody or control. A single hard drive is capable of storing the equivalent of literally thousands of pages of documents, and thus the volume of information possessed by a corporation with several thousand employees is staggering. In addition, electronic information is very mutable. In many instances, it can be altered or deleted with a few simple keystrokes. Accordingly, when a corporation finds itself in litigation, a single discovery request has the potential to become a nightmare.

Requests for electronic discovery generally have the potential to lead to sanctions in two ways: (1) when a respondent fails to produce responsive electronic data, and (2) when a respondent destroys or alters electronic data. Regardless of whether it was done intentionally or not, the failure to produce relevant electronic information or the destruction of such information can have drastic consequences.

This article will examine discovery sanctions under Federal Rule of Civil Procedure Rule 37 in relation to requests for electronic information, and will address some proactive strategies to help avoid the potential pitfalls of electronic discovery.

I. Federal Rule Of Civil Procedure 37

It is well established that the federal discovery rules apply to electronic evidence, including Federal Rule of Civil Procedure 37.² A court has the authority under Rule 37(b)(2) to impose discovery sanctions when a party "fails to obey an order to provide or permit discovery."³ Rule 37(b)(2) provides that "the court in which the action is pending may make such orders in regard to the failure as are just."⁴ The court can issue an order (a) establishing facts; (b) precluding claims or defenses or the introduction of designated matters into evidence; (c) striking pleadings, staying proceedings, or dismissing the action; or (d) finding contempt of court.⁵ Additionally, a court may require the sanctioned party or attorney or both "to pay the reasonable expenses including attorney's fees, caused by the failure, unless the court finds that the failure was substantially justified or that other circumstances make an award of expenses unjust."⁶ Generally, violation of a court order regarding discovery is necessary to trigger the discovery sanctions of Rule 37(b).⁷

Given the vast amount of electronic information retained by the average modern day company, and the relative ease with which that information, either intentionally or otherwise, may be altered or destroyed, it is easy to appreciate the heightened potential for discovery sanctions when responding to requests for electronic information. A court has the ability to impose severe sanctions for improperly failing to produce electronic information, and it is imperative that attorneys take the necessary steps to lessen the chances of such a disastrous result against their clients. The first step is to identify the potential pitfalls to avoid regarding electronic discovery.

A. Sanctions For The Failure To Produce Electronic Evidence

A respondent who fails to produce relevant electronic evidence in response to a discovery request may be sanctioned under Rule 37.⁸ A party also may be sanctioned for failing to produce relevant electronic information in a timely manner.⁹ The sanction must be appropriate and proportionate to the circumstances surrounding the failure to produce the discovery.¹⁰ At a minimum, courts require that the responding party knew, or should have known, that the documents were relevant to pending, imminent or reasonably foreseeable litigation.¹¹

Courts have broad discretion with respect to imposition of sanctions under Rule 37 for the failure to produce evidence.¹² Sanctions can include monetary penalties (such as attorney's fees, and other costs associated with making a motion to compel), exclusion of evidence, adverse inference jury instructions, and dismissal or default judgment.¹³ A monetary penalty or award of reasonable attorney fees and costs is frequently used as a sanction where a party fails to produce electronic data in a timely fashion.¹⁴ Monetary sanctions are less severe and are typically imposed when unnecessary costs are incurred by the party requesting production and considerable time and effort is required by the court.¹⁵

Courts also may impose severe sanctions in certain instances when a party fails to produce electronic information in a timely manner. The most serious sanction utilized by courts is an order which essentially disposes of the case.¹⁶ An adverse inference instruction also is commonly used as a severe sanction.¹⁷ The three criteria for the imposition of an adverse inference instruction for non-production or untimely pro-

duction are: (1) the party had an obligation to produce evidence; (2) the party failed to produce evidence with culpable state of mind; and (3) the missing or destroyed evidence was relevant and would support claim or defense of requesting party.¹⁸ The Second Circuit recently discussed the requisite culpable state of mind to determine whether a party's failure to comply with a discovery request for electronic evidence warrants the imposition of sanctions in *Residential Funding Corp. v. DeGeorge Financial Corp.*¹⁹ In *Residential Funding*, the Second Circuit held that "discovery sanctions, including an adverse inference instruction, may be imposed where a party has breached a discovery obligation not only through bad faith or gross negligence, but also through ordinary negligence."²⁰

Given the low threshold of culpability sufficient to warrant severe sanctions for the failure to produce relevant discovery in a timely manner, it is imperative that attorneys advise their clients to take a proactive approach to electronic discovery. It is not enough for a responding party simply to rely on the fact that they did not intentionally or recklessly fail to meet their discovery obligations. Rather, a party should be prepared to demonstrate that it took reasonable and diligent steps to ensure compliance with the discovery rules.

B. Sanctions For Spoliation Of Electronic Evidence

Spoliation of evidence is the destruction or significant alteration of evidence, or failure to properly preserve evidence for pending or reasonably foreseeable litigation.²¹ When a party demonstrates spoliation, a wide range of sanctions are available. These sanctions include ordering dismissal of the culpable party's suit, entering a default judgment against the culpable party, striking of pleadings, precluding the culpable party from giving testimony regarding the destroyed evidence, or giving an adverse inference instruction to the jury against the culpable party.²² Courts are more likely to impose a severe sanction for spoliation of electronic evidence than when faced with a party's untimely production of relevant documents.²³ The court's authority to impose sanctions for spoliation derives from both Rule 37(b) and from the court's inherent power.²⁴

The threshold question when considering sanctions for spoliation of evidence is whether the party who destroyed the evidence had any obligation to preserve it.²⁵ Essentially, the party should be on notice that litigation was likely to be commenced.²⁶ A party may be put on notice through a discovery request, through the complaint itself, or through notification, prior to the filing of a complaint, that litigation is expected.²⁷ Additionally, a party is bound by any court order to preserve electronic evidence.²⁸ Indeed, many plaintiff's attorneys routinely move for document preservation orders at the time they file a complaint.

Once it is demonstrated that evidence was destroyed by a party with an obligation to preserve it, the court must "consider (1) the degree of fault of the party who destroyed the evidence; (2) the degree of prejudice suffered by the opposing party; and (3) the appropriate sanction."²⁹ When determining the appropriate sanction for spoliation of evidence, courts have broad discretion.³⁰ A proper sanction for spoliation should be designed to: (1) deter the parties from engaging in spoliation; (2) place the risk of an erroneous judgment on the party who wrongfully created the risk; and (3)

restore the prejudiced party to the same position he would have been in absent the wrongful destruction of evidence by the opposing party.³¹

Generally, substantial prejudice and culpability must be present to impose severe sanctions for spoliation of evidence, such as an adverse inference instruction.³² The level of culpability varies among jurisdictions, but usually willfulness, bad faith or fault constitute behavior warranting severe sanctions.³³ As discussed above, the court in *Residential Funding* held that culpability is satisfied by showing that evidence was destroyed negligently, but other courts have held that willful destruction of evidence is required.³⁴ Courts also may focus on whether the lost evidence caused significant prejudice to the requesting party.³⁵ To assess prejudice, a court must determine whether there is any possibility that the destroyed evidence would have been of the nature alleged by the party affected by its destruction.³⁶ The burden falls on the prejudiced party to produce some evidence suggesting that a document or documents relevant to substantiating their claim would have been included among the destroyed files.³⁷ However, actual prejudice is not always a precondition for a severe sanction if the party's conduct is at least negligent and sanctions are necessary to further the remedial purpose of the adverse inference.³⁸

Again, given the relative ease with which electronic information may be altered or deleted, either intentionally or otherwise, attorneys must advise their clients to take all reasonable steps to ensure the preservation of electronic information and comply with the discovery rules. While the unique characteristics of electronic information make it very difficult to guarantee complete preservation and production of all electronic information, companies and their attorneys should undertake several proactive measures to facilitate that goal.

II. Proactive Measures

As set forth above, even inadvertent actions or actions taken in the ordinary course of business with respect to electronic information have the potential to drastically undermine a party's defense or prosecution in litigation. Accordingly, companies and their attorneys need to implement several steps to minimize this risk. The first precautionary step should begin prior to and regardless of the threat of any imminent litigation.

A. Electronic Document And E-mail Retention Policies

Typically, the destruction of electronic documents does not result in sanctions or raise an adverse inference of spoliation if it is done in accordance with a departmental records retention policy without knowledge that the document is relevant to any party in litigation.³⁹ Accordingly, attorneys should advise all their clients to create and implement reasonable electronic document and e-mail retention policies. It is important to remember that document retention periods for certain clients, such as publicly traded companies, financial institutions, accountants or auditors, may be set by regulation or statute. Companies should strictly and consistently comply with their internal retention policies because where documents are inconsistently destroyed, a court may find this to be evidence that the destruction was done in bad faith.⁴⁰ When electronic evidence is altered or destroyed in accordance with an established retention policy prior to the threat of litigation, the imposition of a spoliation sanction for the

destruction of electronic evidence generally requires a showing of a culpable mind and prejudice by the requesting party.⁴¹

However, once a party knows of threatened litigation, courts will impose severe sanctions for destroying electronic evidence even if the party destroyed it in accordance with an established record retention policy.⁴² Accordingly, attorneys should instruct their clients that once litigation has commenced, they must preserve all electronic evidence that may be related to the matter, even materials routinely deleted in the ordinary course of their business and pursuant to an established retention policy. Many computer systems may be configured to regularly delete e-mail or old files, and a party needs to alter these systems and to ensure preservation of these files once it becomes aware of pending litigation.

B. Preservation Of Evidence Letters

As discussed above, the routine purging of electronic information may lead to severe sanctions once a party is on notice of a potential litigation. Many businesses may be unaware that such innocent and routine actions can result in drastic consequences. Accordingly, it is important at the outset of any litigation for an attorney to communicate this potential hazard to his or her clients as early as possible and take steps to ensure the preservation of electronic information. One of the best ways for attorneys to achieve this goal is by routinely sending clients a preservation of evidence letter as soon as possible after being retained for any new litigation.

The preservation of evidence letter should specifically address the preservation of all electronic information, which many times may be overlooked by a client, including all computer files, e-mail files, voice mails, files from any personal data assistants, and any backup or storage files or tapes. In addition, the letter should direct itself to the appropriate personnel at the client's offices. Many times outside attorneys only deal directly with a client's legal department. In these circumstances, the letter should be prepared in consultation with in-house counsel and be directed toward the individuals who are most likely to be in the department that has the actual ability to implement the required document preservation activities, such as utilizing a new or amended record retention policy. This typically is the client's information technology department. The letter should also be directed to individuals who may have copies of relevant electronic records on their home and office personal computers or personal data assistants (PDA's).

C. Familiarity With Electronic Information

The most basic, but arguably the most important, proactive step for attorneys regarding electronic discovery is to learn as much as possible about their client's computer systems and various software and database applications as early as possible in any litigation. An attorney does not need to become a computer expert, but it is essential that he or she obtain a working knowledge of the universe of electronic information in the client's possession, custody or control. It is impossible for an attorney to ensure that the client is not unknowingly exposing itself to an unnecessary and potentially disastrous discovery sanction without first understanding the types of electronic information that may be maintained and therefore may be at issue. The best way to accomplish this step is to schedule an early meeting with in-house counsel and the

individuals most knowledgeable about the client's computer systems. This will often be the client's director of information technology, but it will likely be beneficial to have additional individuals in that department attend at the outset to help ensure that you get a complete and accurate picture of the overall technology environment. In many instances, no one individual has such comprehensive knowledge, and individuals who work with network users on a daily basis often have a more intimate understanding of what types of documents may be encountered than a higher-ranking superior. At a minimum, an attorney needs to ensure that he or she adequately understands the client's computer operating systems, retention policies and procedures, system backup procedures, and storage methods and procedures. Once an attorney adequately understands the electronic information at issue, he or she can work with in-house counsel to properly oversee the discovery process and protect the client from the potential pitfalls created by electronic discovery.

Conclusion

The digital age is firmly upon us. Although technology has greatly improved the ability and efficiency in which attorneys are able to provide quality service to their clients, it also has created the potential for numerous discovery problems. In addition to the ease with which it can be created, electronic information can be altered, transferred or destroyed almost instantaneously, and from remote locations, often with little more than a few keystrokes. These characteristics greatly increase the potential for non-compliance with discovery obligations, which can have very serious consequences in litigation. Accordingly, at a minimum, businesses and their attorneys need to implement a few simple proactive strategies to minimize this risk in litigation, including implementing reasonable electronic document and e-mail retention policies, communicating the company-wide requirement for information preservation during litigation, and ensuring that the attorneys adequately understand the client's computer systems.

ENDNOTES

1. See Wendy R. Liebowitz, *Digital Discovery Starts to Work*, Nat'l L.J., Nov. 4, 2002, at 4.
2. See *Anti-Monopoly, Inc. v. Hasbro, Inc.*, No. 94 Civ. 2120, 1995 WL 649934 (S.D.N.Y. Nov. 3, 1995) ("today it is blackletter law that computerized data is discoverable if relevant").
3. Fed. R. Civ. P. 37(b)(2).
4. Fed. R. Civ. P. 37(b)(2).
5. *Id.*
6. *Id.*
7. See, e.g., *Pennar Software Corp. v. Fortune 500 Systems*, No.01-01734 EDL, 2001 U.S. Dist. LEXIS 18432 at *12 (N.D. Cal. Oct. 25, 2001) (citing *Unigard Sec. Ins. Co. v. Lakewood Eng'g & Mfg. Corp.*, 982 F. 2d 363, 367-68 (9th Cir. 1992); accord *Shepherd v. American Broad, Cos., Inc.*, 62 F.3d 1469, 1474 (D.C. Cir. 1995).

8. *See, e.g., Madden v. Wyeth*, No. 3-03-CV-0167-R, 2003 U.S. Dist. LEXIS 6427, at *4 (N.D. Tex. Apr. 15, 2003).
9. *See Fautek v. Montgomery Ward & Co.*, 96 F.R.D. 141, 145-146 (N.D. Ill. 1982).
10. *See Danis v. USN Communs., Inc.*, No. 98 C 7482, 2000 U.S. Dist. LEXIS 16900, at *94-95 (N.D. Ill. Oct. 20, 2000).
11. *See LEXIS-NEXIS v. Beer*, 41 F. Supp. 2d 950, 954-55 (D. Minn.1999).
12. *See Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99, 106 (2d Cir. 2002)
13. *See, e.g., LEXIS-NEXIS*, 41 F. Supp. 2d at 954. The court's menu of sanctions include: "(1) an order that the matters regarding which the order was made or any other designated facts shall be taken to be established for the purposes of the action" and (2) an order requiring "the party failing to obey the order or the attorney advising that party or both to pay the reasonable expenses including attorney's fees, caused by the failure." *Id.*
14. *Id.*
15. *See, e.g., Pastorello v. New York City*, No. 95 Civ. 470, 2003 U.S. Dist. LEXIS 5231, at *40-41. (S.D.N.Y. Mar. 31, 2003)
16. *See Thomas v. Bombardier-Rotax Motorenfabrick*, 909 F. Supp. 585, 589 (N.D. Ill. 1996).
17. *See, e.g., Residential Funding Corp.*, 306 F.3d at 106.
18. *Id.* at 111-13.
19. *Id.* at 101 (vacating jury verdict and remanding for reconsideration of whether plaintiff's failure to timely or fully produce e-mail back-up tapes warranted adverse jury instruction).
20. *Id.*
21. *See West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 779 (2d Cir. 1999).
22. *See Rush v. Artuz*, No. 00 Civ. 3436, 2003 U.S. Dist. LEXIS 7158, at *5 (S.D.N.Y. Apr. 3, 2003).
23. The destruction of electronic evidence is difficult because deleted electronic data often is recoverable from a computer system with the assistance of specially designed software. However, companies have developed and are marketing software specifically designed permanently to purge all traces of electronic evidence from a computer system. The mere fact that a party possesses such purging software, however, can lead to harsh sanctions in light of a litigant's duty to preserve evidence. *See Kucala Enterprises, Ltd. v. Auto Wax Co., Inc.*, 2003 WL 21230605 (N.D. Ill. May 27, 2003) (dismissing claim and assessing fees and costs against party that downloaded electronic evidence destruction software).
24. *See, e.g., Residential Funding Corp.*, 306 F.3d at 106-07.
25. *See Rush*, 2003 U.S. Dist. LEXIS 7158, at *6.
26. *Id.*
27. *Id.*

28. *Id.* at *6-8. In *Rush*, the defendant was bound by a court-ordered stipulation to preserve surveillance videotapes when requested.
29. *Id.* at *8 (citations omitted).
30. *Id.* at *17.
31. *Id.*
32. See *Danis*, 2000 U.S. Dist. LEXIS 16900, at *94-95.
33. See, e.g., *Pastorello*, 2003 U.S. Dist. LEXIS 5231, at *29-31 (stating that the court does not require that the spoliator act in bad faith and the Second Circuit holds that the culpable state of mind is satisfied by showing that the evidence was destroyed knowingly or negligently).
34. See, e.g., *Williams v. CSX Transp., Inc.*, 925 F. Supp. 447, 452 (S.D. Miss. 1996), *aff'd without opinion*, 139 F.3d 899 (5th Cir. 1998) (loss of computer records relating to speed of train in collision was not willful and no bad faith or conduct shown to warrant adverse inference).
35. See *Turner v. Hudson Transit Lines*, 142 F.R.D. 68, 75-76 (S.D.N.Y. 1991)
36. See *Rush*, 2003 U.S. Dist. LEXIS 7158, at *8.
37. *Id.* at *9.
38. See *Turner*, 142 F.R.D. at 75.
39. See, e.g., *Coates v. Johnson & Johnson*, 756 F.2d 524, 551 (7th Cir. 1985).
40. See, e.g., *In re Prudential Ins. Co. of Am. Sales Practices Litig.*, 169 F.R.D. 598, 615 (D.N.J. 1997) (adverse inference from destruction of relevant computer records because document retention policy was haphazard and uncoordinated).
41. See *William T. Thompson Co. v. General Nutrition Corp.*, 593 F. Supp. 1443, 1455 (C.D. Cal. 1984).
42. See *id.* at 1447. ■

**MEALEY'S LITIGATION REPORT:
DISCOVERY**

edited by Cheryl Scott

The Report is produced monthly by



P.O. Box 62090 King of Prussia, Pa, USA
Telephone: (610) 768-7800 Fax: (610) 962-4991
1-800 MEALEYS (1-800-632-5397)
Email: mealeyinfo@lexisnexis.com Web site: <http://www.mealeys.com>