



Starting at 11:00PM Thursday, Jan 30 through 5:00AM on Friday, Jan 31, our Internet Provider will be performing maintenance which may cause the site to be unavailable.

[Home](#) > [News & Publications](#) > [Wisconsin Lawyer](#) > [Article](#)

Wisconsin
Lawyer™

THE OFFICIAL
PUBLICATION OF THE
STATE BAR OF
WISCONSIN VOLUME NUMBER
2004 77 7

YOUR PRACTICE. OUR PURPOSE.
WISCONSINLawyer

[Read/Post Comments](#)

Electronic Evidence in the 21st Century

While existing rules of civil procedure and evidence have been used with some success to manage the electronic revolution to date, they don't go far enough. The author calls for a comprehensive revision of these rules to take into account the many ways electronic evidence is different from paper evidence. Read what counsel can do now until fundamental changes are made.

WILLIAM GLEISNER III

Electronic Evidence in the 21st Century

While existing rules of civil procedure and evidence have been used with some success to manage the electronic revolution to date, they don't go far enough. The author calls for a comprehensive revision of these rules to take into account the many ways electronic evidence is different from paper evidence. Read what counsel can do now until fundamental changes are made.

Sidebars:

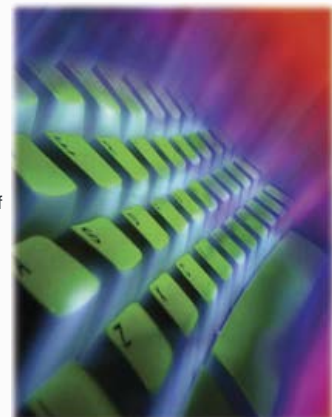
- [Definition of Terms](#)
- [Sample Motion for Sanctions for Failure to Produce Evidence](#)

by *William C. Gleisner III*

It is refreshing to be able to cite authorities from the last century ... and to experience the rare and unusual assurance that, in some ways, the law changes slowly or not at all."¹

When it comes to electronic evidence, it seems that "the law changes slowly or not at all." The bench and bar have for the most part elected to deal with electronic evidence by subjecting it to rules that were created to solve the problems of a paperbound world. While the existing rules of civil procedure and evidence have been used with some measure of success to manage the electronic revolution to date, we must fundamentally modify our procedural and evidentiary rules so that they are responsive to our electronic world. This article only addresses electronic evidence in civil proceedings.

Because of the pervasiveness of electronic data, a piecemeal approach to making the needed changes will not do. We also should not wait for the common law to afford solutions. Many of the issues regarding electronic evidence are complicated and technical, and individual courts working through the common law cannot be expected to retain the technical experts or engage in the probing technical analysis needed to develop consistent responses to all of the many problems electronic evidence presents today. We must have uniform and consistent rules that are developed after thoughtful deliberation by respected institutions that understand the legal issues and can afford to retain the needed technical advisors. The rules that are adopted should be based upon and



Live 1

informed throughout by sound technical analysis.

What is needed is a national conference comparable to but more comprehensive than the National Conference of Commissioners on Uniform State Laws (NCCUSL) that produced the Uniform Commercial Code (UCC).² The time has come for the American Bar Association, the Judicial Conference of the United States,³ state institutions such as the Wisconsin Judicial Council,⁴ law schools, and other "think tanks" to come together to undertake a comprehensive revision of the rules of both civil procedure and evidence to take account of the many ways in which electronic evidence is unique and is different from paper evidence. Just in terms of the rules of civil procedure governing electronic discovery, Chief Justice Shirley Abrahamson recognized the need for such an undertaking in a concurring opinion of a case that was decided just before this article went to press.

"I also write to comment on the issue of production of electronic information. ... In 2004, most information is kept in digital form, and discovery, preservation, and production of electronic information is one of the leading legal issues facing not only corporate America but also government. Reform in discovery, including electronic discovery, is a priority.... This court has not previously confronted the issue of discovery of electronic data. ... The volume, number of storage locations, and data volatility of electronically stored information are significantly greater than those of paper documents. In addition, electronic information contains non-traditional types of data including metadata, system data, and 'deleted' data. Furthermore, the costs of locating, reviewing, and preparing digital files for production may be much greater than in conventional discovery proceedings. ... The majority opinion does not recognize the special problems [regarding the] production of electronic information or give guidance to the judge or the parties about these unique issues."⁵

This article addresses some of the changes that ought to be considered by a national conference. The article also addresses what counsel can do until fundamental changes are made in our rules of civil procedure and evidence. Given the present paperbound rules, defense counsel must devise ad hoc workable, cost effective, and defensible guidelines for determining which items of electronic evidence must be preserved and by what means. Defense counsel also need to determine how they will search for electronic evidence, produce what is reasonable, and resist requests that are unreasonable. Plaintiffs, on the other hand, need to develop strategies within the context of the present paperbound rules for discovering electronic evidence and laying a proper foundation for its use and admissibility at trial.

Electronic Evidence Is Indeed Different

One think tank, the Sedona Conference (the Conference),⁶ has begun to address electronic evidence in a comprehensive fashion, and its work can serve as a template for revisions in the rules of civil procedure and evidence. The Conference has recently issued a report, *The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production* (January 2004),⁷ in which the authors identify characteristics that make electronic evidence different from paperbound evidence.

The many qualitative and quantitative differences between producing electronic documents and producing paper documents can be grouped into six broad categories:

- 1) **Volume and Duplicability.** There are vastly more electronic documents than paper documents, and electronic documents are created at a much greater rate than paper documents.
- 2) **Persistence.** Electronic documents are more difficult to dispose of than paper documents. This persistence of electronic data compounds the rate at which electronic data and documents accumulate and results in the existence of an entire subset of electronic data that may be unknown to the individuals with ostensible custody over it.
- 3) **Dynamic, Changeable Content.** Computer information, unlike paper, has dynamic content that is designed to change over time even without human intervention.
- 4) **Metadata.** Electronic documents, unlike paper, contain information about the document or file that is recorded by the computer to assist in storing and retrieving the document or file at a later date.
- 5) **Environmental Dependence and Obsolescence.** Electronic data, unlike paper data, may be incomprehensible when separated from its environment.
- 6) **Dispersion and Searchability.** While an employee's paper documents will often be consolidated in a few filing cabinets, the employee's electronic documents could reside in many locations: desktop hard drives, laptop computers, network servers, floppy disks, and backup tapes.⁸

Courts Lack Rules and Consistency for the Electronic Revolution

Some local courts have adopted creative rules and well-thought-out decisions to deal with the electronic revolution.⁹ However, most courts have struggled with electronic data, seemingly trying to put a square peg in a round hole.

Courts are not unaware of the importance of the electronic world; however, their responses only address a part of the problem and there are no consistent efforts to come to terms with the electronic world.

Many courts strive to make documents and case information available online. For example, the Wisconsin Supreme Court makes appellate information available via its WSCCA.1 Web site¹⁰ and trial court information is available via the Wisconsin Circuit Court Access system (CCAP).¹¹ On the federal level, electronic records can be retrieved via the PACER system.¹² It's also true that some courts, such as the U.S. District Court for the Western District of Wisconsin,¹³ supply lawyers with user friendly courtroom technology and encourage the use of electronic evidence and the filing of briefs and other documents electronically. Some courts, such as the U.S. District Court for the Northern District of Ohio, insist that all documents must be filed electronically unless good cause is shown why that isn't possible.¹⁴ Many courts, however, do not address the issue of electronic documents in their rules.¹⁵

What is missing are consistent, comprehensive standards and sets of local and national rules that deal with electronic evidence. True, there does appear to be a recognition that change is necessary. The ABA has created an Electronic Discovery Task Force¹⁶ and has made some tentative efforts to draft electronic discovery standards.¹⁷ The Judicial Conference of the United States, which is charged with revising the Federal Rules of Civil Procedure and Evidence,¹⁸ has

begun to study aspects of electronic litigation.¹⁹ While the Judicial Conference is aware of the Internet's impact on the courts,²⁰ however, it appears that the Judicial Conference only intends to modify some of the Rules of Civil Procedure governing electronic discovery, and any proposed rules will not even be available for public comment until late summer 2004.²¹ There is no indication that the Judicial Conference intends to address rules governing the admissibility of electronic evidence.

The Sedona Conference Model

As noted above, there is one bright spot on the horizon and that is the Sedona project. The Sedona Principles²² contain an excellent and thoughtful discussion of electronic document management, and they could well serve as a basis for a comprehensive re-evaluation of the rules of civil procedure and evidence. The primary shortcoming of the Sedona approach is its tacit acceptance of the status quo paperbound rules.

There are too many ways in which the current rules of civil procedure and evidence simply do not meet the needs of an electronic universe. Rather than analogizing from existing rules, the often novel issues presented by electronic litigation should be directly addressed.

Admissibility of Electronic Evidence. In terms of the rules of evidence, from the introduction of previously arcane global positioning system (GPS) tracking devices²³ to the introduction of the metadata²⁴ from electronic email, the courtroom will be a very different place in coming years.

Some evidentiary rules already contain references to electronic documents. For example, Wis. Stat. section 910.01(3) specifies that an "original" writing includes "data ... stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately. ..." The foregoing is just a token acknowledgement of the electronic universe. From a careful reading of the online Sedona materials and given the unique nature of electronic evidence, one can infer that a number of revisions to the rules of evidence ought to be considered with respect to the following issues (due to space limitations, only the Wisconsin Rules and not their federal counterparts or existing federal gloss are discussed).

1. What is the evidentiary status of electronic document metadata? What is the evidentiary status of email components, such as headers and routing information?
2. Can a public record be proved within the meaning of Wis. Stat. section 910.05 merely because it appears on a public Web site?
3. How are voluminous electronic documents to be summarized within the meaning of Wis. Stat. section 910.06?
4. What constitutes "personal knowledge" or "lay opinion" under Wis. Stat. sections 906.02 and 907.01, when dealing with information that has been derived from email or other computerized communications?
5. Under what circumstances is an email or some other electronic document a present sense impression, an excited utterance, or a recorded recollection within the meaning of Wis. Stat. section 908.03?
6. Should Wis. Stat. section 908.01 be modified to make it clear when email and other electronic documents are to be construed as admissions by party opponents (or statements against interest) within the meaning of Wis. Stat. section 908.045(4)?
7. Under what circumstances are computer data collections considered records of regularly conducted activity within the meaning of Wis. Stat. section 908.03(6)? Under what circumstances is the absence of an entry in a computer record admissible under Wis. Stat. section 908.03(7)?
8. What is the status under Wis. Stat. section 908.03(17) and (18) of market reports, commercial publications, and learned treatises that are online?
9. What is the status of Web sites and information contained on Web sites, particularly public Web sites, under, for example, Wis. Stat. section 908.03?
10. Is hearsay within hearsay possible under Wis. Stat. section 908.05 in the case of email?
11. How does one handle attacks on and support the credibility of a declarant within the meaning of Wis. Stat. section 908.06 when the hearsay statement is contained in an email?
12. Can public documents, official publications, newspapers, commercial paper, and related documents located on Web sites be self-authenticated under Wis. Stat. section 909.02? Can health care records that are made available on a Web page be self-authenticated under Wis. Stat. section 909.02(11)?
13. Within the meaning of Wis. Stat. section 910.04, how are duplicates or copies in the possession of the opponent handled when they are electronic?
14. In addition to the provisions of Wis. Stat. section 910.01(3), mentioned above, should other examples of authentication or identification be added to Wis. Stat. section 909.015 (such as Internet service provider IDs, email header information, router information, and so on)?
15. How do we deal with facts or data relied upon by an expert under Wis. Stat. section 907.03, when they are located on transient Web sites or other transitory electronic data or are based on volumes of unindexed or poorly indexed electronic data? What are the standards for forensic computer experts' testimony,²⁵ and when should the court call upon the services of a court-appointed computer expert under Wis. Stat. section 907.06?
16. What is the status of computer-generated records that contain the output of computer programs, untouched by human hands, such as log-in records from Internet service providers, telephone records, and ATM receipts? In such a case, should the rules be modified because the evidentiary issue is no longer whether a human's out-of-court statement was truthful and accurate (a question of hearsay), but instead whether the computer program that generated the record was functioning properly (a question of authenticity)?²⁶
17. In email communications, at what point and under what circumstances does the lawyer-client privilege attach within the spirit of Wis. Stat. section 905.03?
18. Are there any circumstances within the spirit of Wis. Stat. section 902.01 in which a judge may take judicial notice of information posted on Web sites, particularly public sites?
19. What role should circumstantial evidence play in establishing the authorship and authenticity of a computer record?
20. How does one establish that computer business records should be admissible because a) they are kept pursuant to a routine procedure designed to assure their accuracy; b) they are created for motives that tend to ensure accuracy (for example, not including those prepared for litigation); and c) they are not themselves mere accumulations of hearsay?

Discovery of Electronic Evidence. Again, the rules of civil procedure governing discovery already contain some references to electronic documents. For example, Wis. Stat. section 804.09(1) specifies that a request to produce documents shall be construed as applying to "writings, drawings, graphs, charts,

photographs, phono-records, and other data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable forms." Carefully thought out revisions to the rules of civil procedure governing discovery must be considered because several courts have expressed frustration with existing solutions to the problem of electronic discovery. For example, the court made the following observation regarding efforts to discover an adversary's computer backup tapes in *McPeck v. Ashcroft*²⁷:

"There is certainly no controlling authority for the proposition that restoring all backup tapes is necessary in every case. The Federal Rules of Civil Procedure do not require such a search, and the handful of cases are idiosyncratic and provide little guidance. The one judicial rationale that has emerged is that producing backup tapes is a cost of doing business in the computer age. ... But, that assumes an alternative. It is impossible to walk ten feet into the office of a private business or government agency without seeing a network computer, which is on a server, which, in turn, is being backed up on tape (or some other media) on a daily, weekly or monthly basis. What alternative is there? Quill pens?"²⁸

One of the chief complaints of defendants is that expansive electronic discovery imposes an unfair burden on them. Defendants claim that the cost of extensive electronic discovery should be shifted from them to the plaintiff. In *Zubulake v. UBS Warburg LLC*,²⁹ the court stated: "[C]ost-shifting should be considered only when electronic discovery imposes an 'undue burden or expense' on the responding party. The burden or expense of discovery is, in turn, 'undue' when it 'outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues."³⁰

The *Zubulake* court proceeded to analyze the requested electronic evidence in terms of accessibility, a task that would have been made much easier if the discovery rules spelled out in some detail what is and what is not "accessible data" for discovery purposes. The court stated that the following standards should be considered when a defendant requests cost-shifting in the case of electronic discovery:

1. The extent to which the request is specifically tailored to discover relevant information;
2. The availability of such information from other sources;
3. The total cost of production, compared to the amount in controversy;
4. The total cost of production, compared to the resources available to each party
5. The relative ability of each party to control costs and its incentive to do so;
6. The importance of the issues at stake in the litigation; and
7. The relative benefits to the parties of obtaining the information.³¹

Other courts have been forced to create their own sets of similar guidelines from whole cloth.³² Courts and counsel need new, comprehensive discovery rules. As noted above, Wisconsin Chief Justice Abrahamson has recently said as much. The general scope of the type of needed discovery rules appears in the next section of this article.

How Should a Defendant Prepare for and Respond to Electronic Discovery Requests?

Given the present paperbound status of discovery rules, a defendant will find little consistent guidance in either federal or state case law. However, defendants would be well advised to carefully study the Sedona Principles,³³ discussed earlier. The Sedona authors (consisting mainly of lawyers and corporations concerned with antitrust, complex litigation, and intellectual property rights), have distilled their primary principles into a single page.³⁴ However, the Sedona Principles are annotated in a detailed 40-page exposition³⁵ that can be used by any defendant as a basis for coming to grips with electronic discovery issues, at least until the courts create definitive rules. These principles could also form the starting point for a comprehensive set of discovery rules. The principles are set forth here so that defense counsel can appreciate their breadth and comprehensiveness.

The Sedona Principles

1. Electronic data and documents are potentially discoverable under Fed. R. Civ. P. 34 or its state law equivalents (in Wisconsin, Wis. Stat. section 804.09(1)). Organizations must properly preserve electronic data and documents that can reasonably be anticipated to be relevant to litigation.
2. When balancing the cost and burden of and need for electronic data and documents, courts and parties should apply the balancing standard embodied in Fed. R. Civ. P. 26(b)(2) and its state law equivalents, which require considering the technological feasibility and realistic costs of preserving, retrieving, producing, and reviewing electronic data, as well as the nature of the litigation and the amount in controversy.
3. Parties should confer early in discovery regarding the preservation and production of electronic data and documents when these matters are at issue in the litigation and seek to agree on the scope of each party's rights and responsibilities.
4. Discovery requests should make as clear as possible what electronic documents and data are being asked for, while responses and objections to discovery should disclose the scope and limits of what is being produced.
5. The obligation to preserve electronic data and documents requires reasonable and good faith efforts to retain information that may be relevant to pending or threatened litigation. However, it is unreasonable to expect parties to take every conceivable step to preserve all potentially relevant data.
6. Responding parties are best situated to evaluate the procedures, methodologies, and technologies appropriate for preserving and producing their own electronic data and documents.
7. The requesting party has the burden on a motion to compel to show that the responding party's steps to preserve and produce relevant electronic data and documents were inadequate.
8. The primary source of electronic data and documents for production should be active data and information purposely stored in a manner that anticipates future business use and permits efficient searching and retrieval. Resort to disaster recovery backup tapes and other sources of data and documents requires the requesting party to demonstrate need and relevance that outweigh the cost, burden, and disruption of retrieving and processing the data from such sources.
9. 9) Absent a showing of special need and relevance, a responding party should not be required to preserve, review, or produce deleted, shadowed, fragmented, or residual data or documents.

10. A responding party should follow reasonable procedures to protect privileges and objections to production of electronic data and documents.
11. A responding party may satisfy its good faith obligation to preserve and produce potentially responsive electronic data and documents by using electronic tools and processes, such as data sampling, searching, or the use of selection criteria, to identify data most likely to contain responsive information.
12. Absent agreement of the parties or order of the court, there is no obligation to preserve and produce metadata unless it is material to resolving the dispute.
13. Absent a specific objection, agreement of the parties, or order of the court, the reasonable costs of retrieving and reviewing electronic information for production should be borne by the responding party, unless the information sought is not reasonably available to the responding party in the ordinary course of business. If the data or formatting of the information sought is not reasonably available to the responding party in the ordinary course of business, then, absent special circumstances, the costs of retrieving and reviewing such electronic information should be shifted to the requesting party.
14. Sanctions, including spoliation findings, should only be considered by the court if, upon a showing of a clear duty to preserve, the court finds that there was an intentional or reckless failure to preserve and produce relevant electronic data and that there is a reasonable probability that the loss of the evidence has materially prejudiced the adverse party.

As mentioned above, the main deficiency in the Sedona approach is its assumption that no new rules are needed to deal with electronic discovery. In fact, new electronic discovery rules are needed desperately, and the above Sedona principles and recent case law (such as *Zubulake*) can be used as a foundation for creating such rules.

How Should a Plaintiff Prepare for and Conduct Electronic Discovery?

The author wishes to provide both practice tips and suggested [model discovery](#)  32 KB for use by plaintiffs when conducting electronic discovery.

First, a word of caution to the plaintiffs' bar; today, the ability to conduct electronic discovery is not just useful. The failure to conduct electronic discovery in a wide variety of cases is very likely to lead to charges of professional negligence.³⁶ Unfortunately, many plaintiffs' litigators still think of litigation and discovery in terms of a "paper chase." The world is going electronic, however, and chasing paper will soon lead plaintiffs' litigators down a road marked by missed opportunities, overlooked smoking guns, disappointed clients, and malpractice; the days of the dinosaur litigator are numbered.³⁷ Even where information exists primarily in hard copy, in today's word processing world there undoubtedly are electronic copies or drafts of that hard copy that tell an interesting story about its history.

Electronic discovery should be seriously considered in many types of litigation, including: products liability; negligence actions involving misuse of products;³⁸ medical malpractice or other professional negligence actions; insurance bad faith litigation; negligence or discrimination litigation against municipal corporations; investment negligence or fraud litigation; dealership disputes under Wis. Stat. chapter 135; other business tort litigation; and Title VII, ADA, or 42 U.S.C. section 1983 litigation. In fact, any time documentary evidence is likely to exist in an electronic form, you should consider conducting electronic discovery.

A Plaintiff's Electronic Discovery "Laundry List"

Most plaintiffs' litigators operate on a tight budget. Nevertheless, there are several steps that will enhance the chances of uncovering the existence of electronic evidence and forcing its disclosure without breaking your budget. Plaintiffs' trial attorneys may wish to consider these steps:

- 1) Send out a letter before or immediately after a lawsuit is commenced demanding that all electronic evidence be segregated and preserved. If there is reason to believe the demand will not be complied with, seek a protective order under Wis. Stat. section 804.01(3).
- 2) Before the lawsuit is commenced, preserve evidence that exists on any corporate Web site by downloading its contents to the authoring version of Adobe Acrobat[®].³⁹
- 3) Early in a lawsuit, serve interrogatories that seek just information about the defendant's computer systems. These interrogatories should seek to carefully define possible sources of electronic evidence and inquire whether those sources exist on a defendant's computer system and where they are stored. Also inquire as to what software programs the defendant is using (including all of the technical specifications regarding the same), and request the user and administrator manuals for all relevant software that are not available commercially.
- 4) Learn who does the computer work for a corporate defendant (that is, its information service ["IS"] officers) by use of the foregoing interrogatories or through a Wis. Stat. section 804.05(2)(e) deposition (equivalent to an F.R.C.P. 30(b)(6) deposition). After discovering who did and/or does the computer work for a defendant, depose those individuals.
- 5) Serve a second set of interrogatories that seeks disclosure of facts and evidence, and include in that set a separate section that specifically seeks disclosure of relevant electronic evidence. When you seek electronic discovery, ask that any evidence that exists in electronic format be provided to you just as it exists in the defendant's computer systems. This may occasion some battles relating to format, metadata, privilege, convenience, and cost. So, you might postpone insisting on productions in native format until you have reviewed what the defense is willing to give you without a battle. However, ideally you want evidence that exists electronically to be provided in the native electronic format if at all possible, instead of just receiving hard copies or .pdf⁴⁰ or .tiff⁴¹

William C. Gleisner III, Marquette 1974, is a former officer and member of the Board of Directors of the Wisconsin Academy of Trial Lawyers. He currently serves as chairperson of the Academy's Amicus Curiae Committee. He practices in Milwaukee as Of Counsel to the law firm of Kersten &



McKinnon and has an extensive background in both state and federal litigation. Mr. Gleisner's focus for the past six years has largely been on the technical and legal aspects of obtaining, organizing, and managing electronic evidence. He has provided computerized litigation support and "of counsel" assistance to several law firms throughout the United States, helping them to plan, formulate, and execute electronic discovery strategy. He is a Summation Certified Trainer, and formerly was both a Microsoft Certified Systems Engineer and a Citrix Certified Administrator.

Copyrighted 2004, William C. Gleisner, III. All rights reserved.

versions of the evidence.


- a) Review all evidence received, in hard copy or in electronic format, quickly (to avoid charges that you have slept on your rights) so that you can make follow-up requests for a native format production if necessary.
- b) Evidence that is provided in .pdf or .tiff format is a good start (and will provide you with a good deal of flexibility in dealing with electronic evidence) if it is organized and labeled so that you can import it into a text and file indexer, such as the DT-Search indexer discussed below. When you receive evidence in .pdf or .tiff formats, review it quickly to determine: i) if it is responsive to your discovery requests; and ii) if it is labeled in a manner that will enable you to index it in a meaningful way.
- c) If the case is important enough, don't settle for email productions in hard copy or .pdf format. Seek to get the metadata⁴² that is associated with email productions. If you don't have the email program that was used to send and receive the discovered email and if it is not available commercially, make a demand for a copy of the software.
- 6) Once you have obtained electronic evidence, you will need to organize and manage it so you can easily search and retrieve information. You can use high-end and expensive programs such as Concordance[®], Summation[®], or Trial Director[®] to accomplish this task, or you can use a relatively inexpensive program like DT-Search[®].⁴³
- 7) If you can make a credible demonstration that crucial electronic evidence is being withheld, you may wish to seek sanctions. The federal courts have relatively extensive experience with sanctions for failures to allow electronic discovery. Some examples of cases in which sanctions have been successfully sought in the context of an electronic discovery dispute are discussed in the sidebar "Sample Motion for Sanctions for Failure to Produce Evidence."
- 8) If you believe significant electronic evidence exists that is being withheld from you and "the game is worth the candle," then you may wish to retain a forensic computer expert to help you pursue more discovery. Such a move is expensive and should only be considered if you really believe there is buried evidence.⁴⁴
- 9) If the case is big enough, you may also wish to seek on-site inspection of a defendant's computer system and, possibly, the appointment of a special master or court-appointed expert witnesses who can independently inspect the defendant's system.⁴⁵ Federal courts have a procedure for setting up such inspections, and you may want to rely on federal authority⁴⁶ to argue that you should be allowed to have such an inspection conducted in state court.

The Duty of a Defendant and Its Counsel to Avoid Spoliation

Writing a letter or otherwise putting a defendant on notice of your intention to seek electronic discovery is not an idle gesture. Spoliation is the destruction of or failure to preserve and protect evidence.⁴⁷ A party has the duty to protect and preserve evidence once it is on notice that it must do so.⁴⁸ A court may well order the preservation of computerized data during the pendency of a lawsuit.⁴⁹ Spoliation of electronic evidence can have very severe consequences.⁵⁰ Courts have held that a party may be under a duty to prevent spoliation even if litigation is only reasonably anticipated.⁵¹


Related to spoliation is the issue of incomplete or inaccurate responses to discovery requests. A sidebar accompanying this article contains a discussion from one of the author's briefs in support of a successful motion for sanctions for failure to produce accurate and complete electronic evidence in a significant products liability action.

Interrogatories Seeking Computer System Information

If you suspect the existence of electronic evidence, you should serve initial interrogatories that seek only information about the nature of the environment in which that evidence resides. These interrogatories should include questions about the defendant's computer system and the names, addresses, and so on, of people who are responsible for managing the various parts of the defendant's computer system (for example, the webmaster, the network administrator, and/or the email administrator). These initial interrogatories seeking information about a defendant's computer system are only as good as the definitions section of the interrogatories.⁵² When creating the definitions section, one may wish to consider using definitional language similar to that located in "[Discovery of Computer Information - Definitions](#)"  104 KB." This definition section is intended to specify as much as possible the elements of a defendant's computer system in which you may have an interest.

In preparing interrogatories seeking information about the defendant's computer system, keep in mind that there may be several things you don't know about the defendant's computer system, and that you can't begin to ask intelligent questions regarding electronic evidence until you have educated yourself. Therefore, it is crucial that you request user and administrator manuals that the defendant uses in administering its computer system.

Suggested Interrogatories and Requests to Produce Information about a Defendant's Computer System

In "[General Interrogatories Regarding the Defendant's Computer System](#)"  46 KB, you will find some of the interrogatories seeking information about a defendant's computer system that this author prepared recently for use in products liability actions. They are not complete, and they need to be revised to reflect the facts of each case, but they may provide you with some ideas for your own interrogatories.

Interrogatories Seeking Discovery of Electronic Evidence

If you think there is relevant electronic evidence, don't hesitate to seek its production just because you have been provided with hard copy versions of that evidence; delay can result in a denial of a later motion to compel discovery.⁵³ When you seek discovery of electronic information, you should: 1) provide a very specific and detailed request that includes a statement of why the information is important to your case;

- 2) expressly request electronic documents by type; and 3) specify the production format that you seek. For example, if you have a good reason to obtain

evidence in .pdf or .tiff format, ask for the evidence in that format. Based on the author's experience, you should seek to obtain electronic evidence in its native format.

You can expect resistance when you seek to obtain electronic evidence in its native format (as opposed to .pdf or .tiff format). Defendants may claim that it is burdensome for them to review all electronic productions for privileged information or metadata, and may even claim that they have an ethical duty not to disclose information in native format.⁵⁵ That is why you must go to considerable pains to review the information that is furnished to you in hard copy, .pdf, or .tiff formats before seeking a native format production. You need to be in a position to make a credible argument to the court that there may be hidden information or other metadata that you can only discover by seeing the data in its native format. Of course, unless you are prepared to spend serious money on forensic computer experts, don't carry the metadata argument too far;⁵⁶ certain metadata and hidden files, such as deleted text,⁵⁷ can only be pursued and analyzed meaningfully with the aid of a forensic computer expert.

After you have carefully reviewed the evidence that the defendant has furnished willingly, and if it appears suspicious, ask that it be produced in its native format just as it exists in the defendant's computer systems. There is older authority that supports such a request. In *DCA Inc. v. Resorts International*,⁵⁸ the court stated:

"The party who is offering [business] records for investigation in lieu of answering an interrogatory should offer them in a manner that permits the same direct and economical access that is available to the party."⁵⁹

As to all requests for electronic evidence, be certain to request that the defendant specifically state which interrogatory is answered by which piece of evidence.

"It is not sufficient to speculate that an answer may be available [from a mass production of business records]. This is little more than an offer to play the discredited game of blind man's bluff at the threshold level of discovery."⁶⁰

It is not necessary to separate out interrogatories seeking electronic evidence from interrogatories seeking other issue- and fact-specific information. However, when you request information in electronic format, specify that fact. Also, in the definitional section of such interrogatories, it is a good idea to specify what you will accept if the electronic evidence is produced on CD or DVD. For example, one might include the specification with respect to CD or DVD production of discovery contained in "Model Discovery Standards," available with this article online.

Suggested Interrogatories and Requests to Produce Electronic Evidence

"Requests to Produce Information from Databases or Similar Sources" (available with this article online) contains some of the interrogatories this author has used specifically seeking electronic evidence from a defendant's computer system. They are not complete, and they need to be revised to reflect the facts of each case, but they may help you in preparing your interrogatories.

Interrogatories Seeking Production of Copies of Email Messages

Defendants will make strong and persuasive arguments about privileged information that is intermingled among discoverable email. This is because email doesn't come in a set of directories such as one finds in Windows. Like Access files, email lives within a metadata environment that cannot easily be split into small parts. In most cases, email will be contained in Microsoft Outlook or Outlook Express, and to obtain and search all of a defendant's emails you will need to seek production of what is called a .pst file.⁶¹ In any case, when it comes to the production of email in its native environment, you will almost certainly need the services of a forensic computer expert if you are going to seek to search or access a defendant's full email records. Beware; battles over email production are extremely expensive, and you could easily find yourself on the wrong end of an award of costs if your request appears burdensome.⁶²

Once you have reviewed the emails that are furnished to you in hard copy or in .pdf format, and if you find several that are particularly interesting, you may wish to consider asking to see just those emails in their native format so you can inspect their metadata. With the help of a forensic expert, it should be possible to instruct the defense to segregate selected Outlook Express email into separate folders and then export it to removable media as a split .pst file that can then be imported into your version of Outlook or Outlook Express.

Protective and Pull Back Orders

For many savvy defendants, particularly large national or international defendants, the first defense to any electronic discovery request is a demand for a protective order. Often disguised as the defendant's effort to protect trade secrets, the goal is to limit the scope of discoverable information and to place plaintiffs in a box that will prevent them from discussing their case with other plaintiffs who have similar cases.

Obviously, the less restrictive such a protective order is the better. One argument is to point out that the plaintiffs have just as much right to communicate with similarly situated plaintiffs as do the many defense counsel that represent a large national defendant. In a state court action, one should insist on strict adherence to the requirements for a protective order set forth in Wis. Stat. section 804.01(3), especially the provisions of 804.01(3)(a)7.

Defendants also may try to protect themselves by requesting a "pull back" stipulation and order. Under a "pull back" stipulation and order, a defendant seeks to have an agreement in advance that if a privileged document is inadvertently produced, the defendant may call it back and the plaintiffs' counsel cannot use it or rely on it in any way. On the face of it, this appears to be a defensible practice, because defendants will argue that there is no way they can go through every email or electronic document before it is produced searching for privileged material. However, the Wisconsin Supreme Court recently held that "[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, to an opposing attorney in response to a discovery request."⁶³

Conclusion

As Chief Justice Abrahamson recently recognized, electronic evidence is unique and requires new rules and procedures. Piecemeal solutions and inconsistent common law decisions only complicate the difficulties presented by electronic evidence. What is needed is a comprehensive overhaul of the rules of evidence and civil procedure, both in Wisconsin and throughout the country. Until such an overhaul, both counsel and the courts need to carefully consider the unique nature of electronic evidence when deciding on its admissibility and use during trial. Moreover, until such a comprehensive overhaul occurs, counsel must devise ad hoc guidelines and procedures that will ensure the preservation and production of electronic evidence in a manner that is fair, reasonable, and cost effective.

Endnotes

¹ *Quick v. State*, 569 So. 2d 1197, 1199 (Miss. 1990).

² *Cf.* Lockhart & Miles, *Proposed UCC Article 2 Revisions Embrace Paperless Electronic Transactions*, 75 Mich. B. J. 516 (1996).

³ See discussion *infra*. The Judicial Conference is responsible for creating or amending federal rules of civil procedure and evidence and acts pursuant to 28 U.S.C. § 331.

⁴ The Wisconsin Judicial Council proposes rule changes to the Wisconsin Supreme Court pursuant to Wis. Stat. section 758.13.

⁵ *Custodian of Records for the Legislative Tech. Servs. Bureau v. State*, 2004 WI 65, ¶¶ 60-62, 64, ___ Wis. 2d ___, ___ N.W.2d ___.

⁶ See <http://www.thesedonaconference.org/>.

⁷ Located at <http://www.thesedonaconference.org/miscFiles/SedonaPrinciples200401>. A copyrighted PDF copy of the Sedona Principles accompanies this article online at www.wisbar.org/wislawmag/2004/07/gleisner.html [hereinafter Sedona Principles].

⁸ *Id.* at 3-5.

⁹ See the Feb. 13, 2004, Guidelines for Electronic Discovery of the U.S. District Court of Kansas, set forth in the appendix to the law review article by Waxse, "Do I Really Have to Do That?" *Rule 26 (a)(1) Disclosures and Electronic Information*, 10 Richmond J. L. & Tech. 50 (Spring 2004).

¹⁰ <http://old.wicourts.gov/wsccl/>.

¹¹ <http://wcca.wicourts.gov/index.xsl>.

¹² <http://pacer.psc.uscourts.gov/pacerdesc.html>.

¹³ <http://www.wiwd.uscourts.gov/>.

¹⁴ http://www.ohnd.uscourts.gov/Electronic_Filing/electronic_filing.html.

¹⁵ This is particularly true of state court systems. However, many federal courts also lack local rules or guidelines governing the admissibility or discovery of electronic evidence. See, e.g., the Local Rules for the Eastern District of Wisconsin, http://www.wied.uscourts.gov/Local_Rules_New.htm (although the Eastern District has guidelines for electronic filing).

¹⁶ <http://www.abanet.org/litigation/taskforces/electronic/home.html>.

¹⁷ <http://www.abanet.org/litigation/taskforces/electronic/document.pdf>.

¹⁸ <http://www.uscourts.gov/judconf.html>. Judicial Conference procedures for proposing amendments to the Rules of Civil Procedure and Evidence are described at <http://www.uscourts.gov/rules/proceduresum.htm>.

¹⁹ March 2002 Judicial Conference Report, at 5, 10, & 11, <http://www.uscourts.gov/judconf/marc02proc.pdf>.

²⁰ October 2001 Judicial Conference Report, at 39, 43, & 50, <http://www.uscourts.gov/judconf/sept01proc.pdf>.

²¹ The Judicial Conference recently reported that "[t]he Advisory Committee ... approved for publication proposed amendments to Civil Rules 16, 26, 33, 34, 37, and 45 dealing with the discovery of electronically stored information ... The Advisory Committee will now transmit the proposed new rule and amendments to the Committee on Rules of Practice and Procedure, with a recommendation that they be published for public comment in August 2004." See <http://www.uscourts.gov/rules/index.html#judicial0304>.

²² See Sedona Principles, *supra* n.7.

²³ David A. Schumann, *Tracking Evidence with GPS Technology*, 77 Wis. Law. 8 (May 2004), www.wisbar.org/wislawmag/2004/05/schumann.html.

²⁴ See the definition of "metadata" in the accompanying sidebar, "Definition of Terms."

²⁵ See, e.g., *Gates Rubber Co. v. Bando Chem. Indus.*, 167 F.R.D. 90 (D. Colo. 1996).

²⁶ *Cf.* Richard O. Lempert & Steven A. Saltzburg, *A Modern Approach to Evidence* 370 (2d ed. 1983).

²⁷ 202 F.R.D. 31 (D.C. Cir. 2001).

²⁸ *Id.* at 33 (citing *In re Brand name Prescription Drugs Antitrust Lit.*, Nos. 94 C 897, MDL 997, 1995 WL 360526 at *3 (N.D. Ill. June 15, 1995)).

²⁹ 217 F.R.D. 309 (S.D.N.Y. 2003).

³⁰ *Id.* at 318.

³¹ *Id.* at 322.

³² See, e.g., *Medtronic Sofamor Danek Inc. v. Michelson*, 2003 U.S. Dist. LEXIS 8587 (W.D. Tenn. 2003); *Keir v. Unumprovident*, 2003 U.S. Dist. LEXIS 14522 (S.D.N.Y. 2003).

³³ See Sedona Principles, *supra* n.7.

³⁴ *Id.* at 10.

³⁵ *Id.* at 11-50.

³⁶ As long ago as 1996 the ABA/BNA Lawyers Manual on Professional Conduct stated: "[A]dvances in technology are relevant to what constitutes [lawyer] negligence and [a] defendant's failure to use available technology to reduce a known risk could be considered negligence" (quoted in McChrystal & Gleisner, *Laptop Litigation: The Impact of Technology on Litigation*, 72 Wis. Law. 14, 60 n.1 (Sept. 1999)).

³⁷ "It was neither a comet nor a dramatic climactic change that killed off the dinosaurs. They perished because they could not adapt to the digital age." Redish, *Electronic Discovery and the Litigation Matrix*, 51 Duke L. J. 561, 562 (2001).

³⁸ This is the theory of recovery in *Wischer v. Mitsubishi Heavy Indus.*, 2003 WI App 202, ___ Wis. 2d ___, 673 N.W.2d 303.

³⁹ This is not the same as the ubiquitous free Adobe Acrobat reader. Version 6 of Adobe Acrobat[®] authoring software costs approximately \$300 and can be purchased at most computer software stores.

⁴⁰ See the definition of "PDF" in the accompanying definitions sidebar.

⁴¹ See the definition of "TIFF" in the accompanying definitions sidebar.

⁴² See "metadata" in the accompanying sidebar, "Definition of Terms."

⁴³ DT-Search[®] is very powerful but inexpensive software that can be used to index millions of documents quickly and then conduct word searches of them using natural language or Boolean search protocols. A single user license costs about \$300. See <http://www.dtsearch.com/casestudies.html>. For Summation software, see www.summation.com. For Trial Director software, see www.indatacorp.com. For Concordance software, see www.dataflight.com.

⁴⁴ There are several forensic computer experts. A competent local company that specializes in forensic computer work is Digital Intelligence, located in Waukesha. See www.digitalintel.com. An excellent national forensic computer expert is Peter Garza, a former Naval intelligence officer. His company is Evidentdata. See www.evidentdata.com. The Indata Corporation, which makes Trial Director software, also does forensic computer work. See www.indatacorp.com. While this author has not used it, another company that does forensic computer work is Electronic Evidence Discovery. See www.eedinc.com.

⁴⁵ Circuit courts in Wisconsin have the power to appoint expert witnesses. See Wis. Stat. § 907.06 ("The judge may on the judge's own motion or on the motion of any party enter an order to show cause why expert witnesses should not be appointed. ...").

⁴⁶ See, e.g., *Playboy Enterprises v. Welles*, 60 F. Supp. 2d 1050, 1055 (S.D. Cal. 1999).

⁴⁷ See *Estate of Neumann v. Neumann*, 2001 WI App 61, 242 Wis. 2d 205, 626 N.W.2d 821 ("Courts have fashioned a number of remedies for evidence spoliation. The primary remedies used to combat spoliation are pretrial discovery sanctions, the spoliation inference, and recognition of independent tort actions for the intentional and negligent spoliation of evidence. ... Wisconsin has recognized the first two remedies.") See *Sentry Ins. v. Royal Ins. Co.*, 196 Wis. 2d 907, 918-19, 539 N.W.2d 911 (Ct. App. 1995) (upholding trial court's exclusion of evidence related to refrigerator from which party's expert intentionally removed components, thereby precluding testing by opposing party); *Jagmin v. Simonds Abrasive Co.*, 61 Wis. 2d 60, 80-81, 211 N.W.2d 810 (1973) (holding that spoliation inference (against party causing spoliation) is inappropriate when evidence was negligently destroyed, but may be appropriate when destruction is intentional).

⁴⁸ Cf. *Yu Jung Park v. City of Chicago*, 297 F.3d 606, 616 (7th Cir. 2002).

⁴⁹ See, e.g., *In re Cell Pathways Securities Litig.*, 203 F.R.D. 189 (E.D. Penn. 2001); *In re Bridgestone*, 129 F. Supp. 2d 1207 (S.D. Ind. 2001).

⁵⁰ *3M v. Pribyl*, 259 F.3d 587, 606 n.5 (7th Cir. 2001) (court allowed negative inference to be drawn from apparent intentional deletion of information from computer hard drive); *Rodgers v. CWR Constr.*, 33 S.W.3d 506, 510 (Ark. 2000); *Patton v. Newmar Corp.*, 538 N.W.2d 116, 120 (Minn. 1995); *Mudge v. Penguin Air Conditioning*, 633 N.Y.S.2d 493 (1995). See also *Mathias v. Jacobs*, 197 F.R.D. 29 (S.D.N.Y. 2000).

⁵¹ *Gates Rubber Co. v. Bando Chem. Indus.*, 167 F.R.D. 90 (D. Colo. 1996).

⁵² Definitions are always important in interrogatories and requests to produce, because if used properly they can make it possible to craft very specific queries with a great deal of economy, thus avoiding problems with the requirement in many jurisdictions that a party can only ask a limited number of interrogatories without court approval. However, for the reasons stated in this article, in discovering electronic evidence definitions are of much greater importance than ever before.

⁵³ Cf. *Jones v. Goord*, 2002 U.S. Dist. LEXIS 8707 (S.D.N.Y. 2002).

⁵⁴ Despite the fact that one should seek evidence in its native format, you may wish to obtain it in .pdf or .tiff format for several reasons. For example, if you are using Summation[®] it may make sense to obtain .tiff images, because it will be easier to load into older versions of that program. However, be aware that the convenience of receiving evidence in .pdf or .tiff format is probably at the expense of receiving the total picture provided by receiving evidence in its native format. Evidence provided in its native format can always be converted to .pdf or .tiff.

⁵⁵ Brown, *Electronic Discovery*, 52 R.I. B. J. 7 (2003).

⁵⁶There are some documents that you know will be associated with metadata. These include email, word processing documents, and output that is probably from a database (such as spreadsheet compilations of facts).

⁵⁷"Deleted" computer records are often not really deleted. A so-called deleted file is discoverable under F.R.C.P. 34. *Simon Property Group L.P. v. mySimon Inc.*, 194 F.R.D. 639 (S.D. Ind. 2000).

⁵⁸1989 U.S. Dist. LEXIS 13559 (D.C. Penn. 1989).

⁵⁹*Id.* at *6 (citing *Sabel v. Mead Johnson*, 110 F.R.D. 553, 555 (D. Mass. 1986)). *Cf.* Wis. Stat. § 804.08(3) (option to produce business records).

⁶⁰*DCA Inc.*, 1989 U.S. Dist. LEXIS 13559, at *6 (citing *In re Master Key*, 53 F.R.D. 87, 90 (D. Conn. 1971)).

⁶¹A sizeable minority of companies uses Lotus Notes for email, and in that case you would seek production of what is called an .nsf file.

⁶²Regarding cost shifting in cases involving electronic discovery, see *Zubulake*, *Medtronic*, and *Keir*, *supra*; *Byers v. Illinois State Police*, 2000 U.S. Dist. LEXIS 9861, at *35-37 (N.D. Ill. 2002); and *Rowe Enter. v. William Morris Agency*, 2002 U.S. Dist. LEXIS 8303, at *23 (S.D.N.Y. 2002), which set forth the criteria to be considered when shifting costs during electronic discovery. See also the cases cited *supra* n.32.

⁶³*Harold Sampson Children's Trust v. The Linda Gale Sampson Trust*, 2004 WI 57, ¶4, ___ Wis. 2d ___, 679 N.W.2d 794.