

**UNDERSTANDING ELECTRONIC DISCOVERY
AND SOLVING ITS PROBLEMS**

ALISTAIR B. DAWSON

Attorney and Partner

Beck, Redden & Secret, L.L.P.

Houston, Texas

ELECTRONIC DISCOVERY

SYNOPSIS

I. INTRODUCTION	4
A. Various Forms and Types of Electronic Information	7
B. Differences Between Paper and Electronic Evidence	8
II. PRESERVATION	12
A. When Does a Duty to Preserve Arise?	13
B. What are a Litigant’s Preservation Obligations?	18
C. What are Counsel’s Preservation Obligations?	19
D. What Must be Preserved?	22
E. How Should Information Be Preserved?	27
III. PRODUCTION	28
A. What Must Be Produced?	29
B. How Does a Party Produce Information that is “Not Reasonably Accessible?”	30
C. In What Form Must Information be Produced?	33
D. Issues that Arise with Production of Electronic Evidence	35
1. Privilege Review and Waiver	36

ELECTRONIC DISCOVERY

2. Privacy Concerns38

E. Who Must Bear the Costs of Producing Electronic Information?40

IV.SANCTIONS 48

A. Death Penalty Sanctions and Excluding Evidence.....50

B. Instructions.....51

C. *Mastercard* and *Philip Morris*—Spoliation Sanctions in Practice.....53

D. The Federal Rules Propose a Safe Harbor56

V.CONCLUSION..... 57

ELECTRONIC DISCOVERY

I. INTRODUCTION¹

*The world was a far different place in 1849, when Henry David Thoreau opined (in an admittedly broader context) that “the process of discovery is very simple.”*²

So begins the first of five electronic-discovery opinions by Judge Shira A. Scheindlin in the *Zubulake* string of cases.³ That a single controversy has given rise to *five* lengthy discussions on electronic discovery augurs that no bright-line

1. The author wishes to acknowledge and thank Connie H. Pfeiffer, an associate with Beck, Redden & Secret, L.L.P., for her contributions to this article.

2. Henry David Thoreau, *A Week on the Concord and Merrimack Rivers* (1849).

3. *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003) (*Zubulake I*) (addressing legal standard for determining cost allocation for producing e-mails contained on backup tapes); *Zubulake v. UBS Warburg LLC*, 2003 U.S. Dist. LEXIS 7940 (S.D.N.Y. 2003) (*Zubulake II*) (addressing reporting obligations); *Zubulake v. UBS Warburg LLC*, 216 F.R.D. 280 (S.D.N.Y. 2003) (*Zubulake III*) (allocating backup tape restoration costs); *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212 (S.D.N.Y. 2003) (*Zubulake IV*) (ordering sanctions for violating duty to preserve evidence); *Zubulake v. UBS Warburg LLC*, 2004 U.S. Dist. LEXIS 13574 (S.D.N.Y. 2004) (*Zubulake V*) (addressing counsel’s duty to communicate discovery obligations to client, particularly in helping client identify sources of discoverable information).

ELECTRONIC DISCOVERY

rules are to be had in this often complicated, costly and contentious area of law. Yet there is hope for more guidance on the horizon. The Federal Civil Rules Advisory Committee has proposed amendments to the federal civil discovery rules to account for the challenges presented by electronically stored information. Once officially promulgated, these rules should provide a national paradigm, laying the foundation for greater uniformity and consensus among the states.

Although a few states, including Texas, have adopted rules to address electronic discovery issues, the federal Civil Rules Advisory Committee recognizes the need for a national consensus:

Adoption of differing local rules by many district courts may freeze in place different practices and frustrate the ability to achieve the national standard the Civil Rules were intended to provide in the areas they address.⁴

Since a national standard does not yet exist, this paper focuses on Texas law, where developed, and turns also to influential opinions from the federal courts. This dual-system approach highlights the need for a national consensus: How could companies that operate interstate and internationally ever hope to meet various discovery requirements in our federal system? Only with a strong

4. Lee H. Rosenthal, Report of the Civil Rules Advisory Committee, May 17, 2004 (available at <www.uscourts.gov/rules>).

ELECTRONIC DISCOVERY

consensus among the jurisdictions will companies and their counsel have confidence that they are upholding their duties.

Accordingly, this paper provides a thorough review of the issues that arise in the presentation and production of electronic discovery, including a review of proposed amendments to the Federal Rules of Civil Procedure. The proposed rules have the benefits of hindsight, in that electronic discovery law has evolved and matured in the last decade. The rules thus reflect the cumulative national efforts of practitioners and judges to address the demands of an electronic era.⁵

Along with a review of the proposed amendments to the Federal Rules, this paper addresses the larger themes presented by discovery, tailoring them to the electronic discovery context. Part II discusses preservation issues, answering questions that should be considered before suit is ever brought: When does a duty to preserve arise? What are litigants' and counsel' preservation obligations? What must be preserved? And how should information be preserved? Part III deals with production issues, addressing what must be produced—even when the requested information is not reasonably accessible, the form in which data must be produced, issues such as privilege review and waiver, and who must bear the costs of production. Finally, Part IV reviews the variety of ways that courts can

5. The proposed federal rules are currently published for comment. The Advisory Committee welcomes the bar to participate in evaluating these proposals, acknowledging that litigants and lawyers live with the problems raised by electronic discovery in ways that judges do not. Comments can be sent electronically to <www.uscourts.gov/rules>.

ELECTRONIC DISCOVERY

police electronic discovery, including death penalty sanctions, exclusion of evidence, and adverse instructions.

But before launching in to these topics, it is useful to review the forms and types of electronic information and the ways electronic data differs from its paper counterpart.

A. Various Forms and Types of Electronic Information

Counsel must be savvy about the myriad devices and places that store electronic data. Beyond the obvious—desktop computers and laptops in the workplace—there are many other places that should be considered when marshalling electronic evidence: personal digital assistants, such as Palm Pilots; home computers; floppy disks; hard drives; CD-ROM devices; backup magnetic tapes; backup storage on the Internet; zip drives; e-mail servers; program files such as word processing documents and computerized spreadsheets; voice-mail; digital cameras; as well as CPU's on various appliances.⁶

Additionally, the Internet presents different types of electronic information. These include web sites, intranets, extranets, cache files (i.e. records of Internet addresses visited by the user), internet browser history files, site log files, bookmarks (i.e. one-click shortcuts created by the user and stored on the user's computer), cookies (i.e. information about the user such as usernames,

6. See Dale M. Cendali & Lydia R. Zaidman, *Electronic Discovery*, 1 Fourth Annual Internet Law Institute 895, 903 (Practicing Law Institute ed., 2000).

ELECTRONIC DISCOVERY

passwords, and preferences, placed in a file by a web-site operator), and directories of cookies on a user's hard drive.⁷

B. Differences Between Paper and Electronic Evidence

The differences between paper and electronic evidence are manifold. These differences affect how lawyers should approach discovery and how clients should prepare for and respond to litigation. A proper understanding of how to approach electronic discovery therefore begins with a framework of the defining characteristics of electronic evidence.

Destructibility: Paper documents can easily be shredded, burned or otherwise permanently destroyed. Not so with electronic evidence. In contrast to paper, digital data is much more difficult to destroy.⁸

Electronic documents and transactions leave a fingerprint on a computer's hard drive, which can often be recovered long after a user presses delete. The delete function merely sends a message that the space occupied by the deleted data is now available to be overwritten by new data. But unless and until new data overwrites every sector of the deleted data (which is scattered randomly

7. See generally Michael Traynor and Lori Ploeger, HOT TOPICS IN ELECTRONIC DISCOVERY, 712 PLI/Pat 51, 55, n. 9-12 (2002).

8. Although digital data is difficult to destroy, it is nonetheless fragile. Entering data, loading software, performing routine maintenance or simply booting a computer can alter files stored on the hard drive. This is discussed further in Part III.E, *infra*.

ELECTRONIC DISCOVERY

about the computer's hard drive), a forensics expert should be able to recover the deleted data.

Volume: While firms and businesses struggle with maintaining on- and off-site physical storage space for paper, electronic documents can be easily created, stored and retrieved. This ease accounts for the exponential difference between the volume of documents stored in file cabinets and warehouses and that of electronic documents stored and maintained on computers. Users tend to save far more information on computers than they ordinarily would simply because computers hold information so conveniently and inexpensively.

The Manual for Complex Litigation illustrates how information stored electronically quickly becomes voluminous:

The sheer volume of [electronic] data when compared with conventional paper documentation, can be staggering. A floppy disk, with 1.44 megabytes, is the equivalent of 720 typewritten pages of plain text. A CD-ROM, with 650 megabytes, can hold up to 325,000 typewritten pages. One gigabyte is the equivalent of 500,000 typewritten pages. Large corporate computer networks create backup data measured in terabytes, or 1,000,000 megabytes: each terabyte represents the equivalent of 500 billion typewritten pages of plain text.

THE MANUAL FOR COMPLEX LITIGATION (4th) § 11.446.

Electronic data may be stored in a number of different locations even within one organization. Data may reside on a central server and also may be

ELECTRONIC DISCOVERY

stored on any number of individual computers. Further, backup tapes may contain electronic data that may or may not exist elsewhere. When some or all of this electronic data becomes potentially discoverable, issues can and will arise as to how to search for potentially discoverable electronic data and who should pay for it. Does every computer in the company need to be searched for potentially responsive information? What about home computers? Text messages, cell phones and PDAs? Where does it stop?

Metadata: Metadata is information about the document itself, or “data about the data.” For example: date, time, sent to, received by, carbon copy (“cc”), blind carbon copy (“bcc”), etcetera. Electronic documents can even reveal valuable information such as who has edited the document, who last accessed the document, and the date and times of those encounters. For better or for worse, this information can make each document tell a story beyond what the document itself says. By contrast, a paper document conveys nothing other than what is written on its face.⁹ Metadata can therefore save the time and money that would ordinarily be entailed in paper discovery by replacing a time-consuming and expensive coding process. Conversely, it can make electronic information versions of information much more appealing to a requesting party on the hunt for the story behind the document.

9. The D.C. Circuit colorfully described this difference between electronic and paper records, noting that the same e-mail, once printed, is not an “identical twin,” but is, at most, a “kissing cousin.” *Armstrong v. Executive Office of the President*, 1 F.3d 1274, 1283 (D.C. Cir. 1993).

ELECTRONIC DISCOVERY

Candor: The spontaneous, unguarded and casual response that electronic communication generates is perhaps the most defining characteristic of the power of electronic evidence in discovery. E-mail, instant messages, and comments sent along with attached documents often reflect a belief that electronic communication is transient and informal. Yet, as discussed above, electronic data is nearly indestructible, and it is these comments that will be introduced in litigation to reveal the unadulterated impressions of an opposing party. Litigants can recreate the circumstances that gave rise to their dispute in the form of offhand opinions, stray remarks, and contemporaneous impressions that would never have appeared in paper documents and formal memorandums. With hopes of capturing this kind of evidence, it is no wonder that parties often seek electronic evidence even at great burden and expense.¹⁰

10. The candor associated with electronic communications provides much fodder for “smoking gun” stories. *See generally*, Strauss v. Microsoft Corp., 814 F. Supp. 1186, 1193-94 (S.D.N.Y. 1993) (detailing evidence of a sexual discrimination claim including sexually-suggestive, and sexually-explicit e-mails). Casual and oftentimes inappropriate use of e-mail has led Kenneth J. Withers, supervising attorney at Conley and Hodge, a Boston litigation-support firm specializing in discovery, to describe e-mail as a “corporate CB radio.” Grossman, *E-Mail Can be Discovered in Litigation: Even ‘Deleted’ Messages Can Come Back to Haunt You*, 96 LWUSA 251 (March 11, 1996).

ELECTRONIC DISCOVERY

II. PRESERVATION

It is well established that electronic evidence is discoverable.¹¹ Although the Federal Rules of Civil Procedure do not currently address the preservation of electronic evidence, businesses are guided by substantive statutory requirements, such as tax and SEC requirements,¹² the general duty to preserve relevant evidence in the face of pending or foreseeable litigation,¹³ and the boundless advice from commentators that—before litigation arises—businesses should implement document retention policies.

11. *Anti-Monopoly, Inc. v. Hasbro, Inc.*, 1995 WL 649934 (S.D.N.Y. Nov. 3, 1995) (“The law is clear that data in computerized form is discoverable even if paper ‘hard copies’ of the information have been produced [T]oday it is black letter law that computerized data is discoverable if relevant.”); *Trevino v. Ortega*, 969 S.W.2d 950, 955 (Tex. 1998) (Baker, J., concurring) (A party may have a statutory, regulatory, or ethical duty to preserve evidence.).

12. *See, e.g.*, The Sarbanes-Oxley Act of 2002 §§ 802, 1519, 1520, 18 U.S.C. 73 (2002) (criminalizing the willful alteration or destruction of records).

13. *Trevino*, 969 S.W.2d at 957 (Baker, J., concurring) (“While a litigant is under no duty to keep or retain every document in its possession . . . it is under a duty to preserve what it knows, or reasonably should know is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery, [or] is the subject of a pending discovery sanction.”) (quoting *Wm. T. Thompson Co. v. General Nutrition Corp.*, 593 F. Supp. 1443, 1445 (C.D. Cal. 1984)).

ELECTRONIC DISCOVERY

The more difficult issues arise before discovery even begins when counsel and client must make decisions about how to fulfill their obligations to preserve evidence for discovery. The nature and volume of electronic evidence call for caution since electronic evidence can be altered or destroyed if not properly preserved. Thus, the obligation to preserve electronic evidence raises several questions: When does a duty to preserve arise? What are litigants' and counsel's preservation obligations? What exactly must be preserved? And how should information be preserved?

These questions are usually prompted by a spoliation complaint. Spoliation refers broadly to the intentional, reckless, or negligent destruction, loss, material alteration, or obstruction of evidence that is relevant to litigation.¹⁴ Once a party complains of spoliation, the threshold question is whether the alleged spoliator was under a duty to preserve evidence.

A. When Does a Duty to Preserve Arise?

Although courts vary in how they describe the temporal aspect of a duty to preserve, the common themes are actual notice and foreseeability. No duty to preserve evidence arises unless the party possessing the evidence has notice of its relevance. *Akiona v. United States*, 938 F.2d 158, 161 (9th Cir. 1991); *Turner v. Hudson Transit Lines, Inc.*, 142 F.R.D. 68, 72-73 (S.D.N.Y. 1991). The complaint may alert the party that certain information is relevant and likely to be

14. The doctrine of spoliation and its application to electronic discovery are discussed more fully in reference to sanctions. *See* Part IV, *infra*.

ELECTRONIC DISCOVERY

sought in discovery. A party is certainly on notice once it has received a discovery request. *Id.* at 73. But notice need not come in the form of a complaint. The duty to preserve could arise *prior* to the time a plaintiff files its complaint if a party is on notice of pending litigation. *Turner*, 142 F.R.D. at 73; *see also Lewy v. Remington Arms Co.*, 836 F.2d 1104 (8th Cir. 1988) (holding the duty to preserve arises where the information is likely to be relevant to foreseeable litigation). Indeed, a party should not be able to subvert the discovery process and the fair administration of justice simply by destroying evidence before a claim is actually filed.¹⁵

15. A number of courts recognize the need for a duty to preserve evidence before a claim is actually filed. *See, e.g., Blinzler v. Marriott Int'l Inc.*, 81 F.3d 1148, 1158-59 (1st Cir. 1996) (holding duty to preserve arose before litigation where defendant hotel destroyed telephone log that would have pinpointed operator's emergency call when defendant knew that guest's spouse had died and that guest had repeatedly attempted to discover when emergency call was placed); *Dillon v. Nissan Motor Co.*, 986 F.2d 263, 267 (8th Cir. 1993) (imposing sanctions where plaintiff destroyed vehicle relevant to litigation in products liability suit); *Welsh v. United States*, 844 F.2d 1239, 1241-42, 1246-48 (6th Cir. 1988) (allowing adverse inference in medical-malpractice case where defendant destroyed skull flap, which should have been sent to pathology laboratory and preserved for litigation since it was only piece of evidence that could establish or refute that doctor was negligent).

ELECTRONIC DISCOVERY

The Texas Supreme Court holds that the duty to preserve arises only when the party knows or should know that there is a substantial chance that a claim will be filed and that evidence in its possession or control will be material and relevant to that claim. *Wal-Mart Stores v. Johnson*, 106 S.W.3d 718, 722 (Tex. 2003); *see also* 1 Weinstein & Berger, WEINSTEIN'S FEDERAL EVIDENCE § 301.06[4] at 301-28.3 (2d ed. 2003) ("There must be a sufficient foundational showing that the party who destroyed the evidence had notice both of the potential claim and of the evidence's potential relevance.").

Johnson was not an electronic discovery case, but it does reveal the Court's position on duty issues, which presumably transcends the type of evidence to be preserved. In this case, Johnson was injured when a store clerk accidentally knocked some decorative reindeer off a shelf and onto his head and arm. *Id.* at 720. At the time of the accident, Johnson complained only of a cut on his arm and indicated to the store clerk that he was otherwise unharmed. Six months later, Johnson sued Wal-Mart for neck pain that allegedly arose out of the reindeer incident and progressively worsened until seventeen months after the incident when Johnson underwent neck surgery. *Id.* By the time Johnson filed suit, Wal-Mart could not produce any of the reindeer because they had all been sold or, if broken, thrown away. *Id.*

Wal-Mart argued, and the Court agreed, that it had no duty to preserve the reindeer as evidence because it had no notice that they would be relevant to a future claim. *Id.* at 722. All the reindeer had been disposed of in the normal course of business, and the store clerk's investigation revealed that Johnson had

ELECTRONIC DISCOVERY

not been seriously injured and had never indicated that he might seek legal relief.

Id. At bottom, Johnson did not sufficiently show that Wal-Mart knew or should have known both of a potential claim and of the evidence's potential relevance.

Importantly, the court did not use an actual knowledge standard to decide whether Wal-Mart had a duty to preserve. The court cited *National Tank Co. v. Brotherton*, 851 S.W.2d 193 (Tex. 1993), as a reference for an objective test to determine when litigation may reasonably be anticipated. *National Tank* defines "anticipation of litigation" in the context of whether a party should be allowed to assert an investigative privilege. Instead of using an actual knowledge standard, *National Tank* recognizes that "common sense dictates that a party may reasonably anticipate suit being filed . . . before the plaintiff manifests an intent to sue." *Id.* at 204. Consequently, the court held that trial courts must consider the totality of the circumstances and decide whether a reasonable person in the party's position would have (or actually) anticipated litigation in order to determine whether the party reasonably anticipated litigation. *Id.* at 207.

The *National Tank* test works in the spoliation context when modified to account for the defensive versus the offensive use of "in anticipation of litigation." In *National Tank*, the party asserting the privilege used the test defensively to shield itself from disclosing privileged information. Naturally, that party had the burden to prove that it subjectively anticipated litigation and that its belief was reasonable. By contrast, spoliation cases deal with parties who offensively use the test to punish another party for its failure to produce evidence. In these cases, the burden is on the nonspoliating party to prove that the spoliating

ELECTRONIC DISCOVERY

party anticipated litigation. Yet this burden is uniquely difficult since it is often difficult to prove that a party subjectively anticipated litigation. And that party, faced with the prospect of sanctions, cannot be relied upon to admit what it subjectively knew. Accordingly, in spoliation cases, a more objective test is in order. Justice Baker articulated this in his concurrence in *Trevino v. Ortega*, stating that:

[A] party should be found on notice of potential litigation when, after viewing the totality of the circumstances, the party either actually anticipated litigation or a reasonable person in the party's position would have anticipated litigation. While in certain circumstances a party may not reasonably foresee litigation until the party is actually notified of the opposing party's intent to file suit, there may be times when certain independent facts will put a party on notice of the potential for litigation. Whether a party actually did or reasonably should have anticipated litigation is simply a fact issue for the trial court to decide by viewing the totality of the circumstances.

Trevino v. Ortega, 969 S.W.2d 950, 956 (Tex. 1998) (Baker, J. concurring).

Consider the work-product privilege discussed in *National Tank* as an especially useful way of self-regulating when the duty to preserve arises. The work-product privilege depends on proof that the materials were prepared in anticipation of litigation. *National Tank*, 851 S.W.2d at 201 (Texas work-product

ELECTRONIC DISCOVERY

privilege (TEX. R. CIV. P. 192.5)); *Admiral Ins. Co. v. U.S. Dist. Ct. for Dist. of Ariz.*, 881 F.2d 1486, 1494 (9th Cir. 1989) (Federal work product immunity (FED. R. CIV. P. 26(b)(3)). Yet if parties anticipate litigation, they fall within the letter and spirit of the cases that hold the duty to preserve arises when litigation is foreseeable. To the extent parties wish to invoke the work-product privilege, they should consider their right to invoke the privilege as triggering a reciprocal duty to meticulously preserve evidence.

B. What are a Litigant's Preservation Obligations?

Judge Shira A Scheindlin's opinion in *Zubulake IV*, 220 F.R.D. at 218, summarizes a litigant's obligations to preserve evidence: Once a party reasonably anticipates litigation, it must implement a "litigation hold" to suspend its routine document retention/destruction and thereby ensure that relevant documents are preserved. A litigation hold will generally not apply to inaccessible backup tapes (i.e. those maintained for disaster recovery purposes). These tapes may continue to be recycled according to company policy. But if backup tapes are accessible (i.e. actively used to retrieve information), then they *would* likely be subject to the litigation hold. One exception to this general rule lies where a company can identify where particular documents are stored on backup tapes. In these cases, *all* tapes storing information of "key players" to the existing or threatened litigation should be preserved if the information contained on those tapes is not otherwise available.

ELECTRONIC DISCOVERY

Once the party implements the litigation hold, counsel must then oversee compliance, monitoring the party's efforts to retain and produce the relevant documents. Doing so ensures that all relevant sources of information are discovered, that relevant information is retained on an ongoing basis, and that relevant non-privileged information is produced to the opposing party.

C. What are Counsel's Preservation Obligations?

The most recent *Zubulake* opinion, *Zubulake V*, 2004 U.S. Dist. LEXIS at *32, extends this discussion to counsel's preservation obligations, emphasizing that counsel has a responsibility to take an active role in helping the client meet its discovery obligations.

Once a litigation hold is in place, counsel must work with the client to ensure that all sources of potentially relevant information are identified and placed "on hold," to the extent required by the client's preservation obligations. To do this, counsel must become fully familiar with her client's document-retention policies and the architecture of that data-retention system. Invariably, the company's Information Technology team must get involved to explain system-wide backup procedures and recycling policy. Counsel must also interview each of the "key players" to the litigation to determine how those individuals habitually stored information.

Should the size of the company or scope of the lawsuit make it infeasible to interview each "key player," counsel can be more creative. The *Zubulake V* opinion suggests that it may be possible to run a system-wide keyword search. *Id.*

ELECTRONIC DISCOVERY

at *34-35. The keyword search should be created broadly, and counsel should preserve a copy of each “hit”—not to review each hit, but only to ensure that those documents are retained. When the opposing party requests documents, the parties can then negotiate a more refined list of search terms to identify responsive documents, and counsel would only be required to review documents that came up as “hits” on the more restrictive search.

The *Zubulake V* discussion thus clarifies that it is *not* sufficient to notify all employees of a litigation hold and expect that the client will then retain and produce all relevant information. Rather, counsel must affirmatively monitor compliance so that all sources of discoverable information are identified and searched.

Additionally, the discovery rules impose a *continuing* duty to supplement disclosures. *See, e.g.*, TEX. R. CIV. P. 193.5(a); FED. R. CIV. P. 26. As the *Zubulake V* opinion explains, the “tricky question” then is what that continuing duty entails.

What must a lawyer do to make certain that relevant information—especially electronic information—is being retained? Is it sufficient if she periodically re-sends her initial “litigation hold” instructions? What if she communicates with the party’s information technology personnel? Must she make occasional on-site inspections?

ELECTRONIC DISCOVERY

Above all, the requirement must be reasonable. A lawyer cannot be obliged to monitor her client like a parent watching a child. At some point, the client must bear responsibility for a failure to preserve. At the same time, counsel is more conscious of the contours of the preservation obligation; a party cannot reasonably be trusted to receive the “litigation hold” instruction once and to fully comply with it without the active supervision of counsel.

Id. at *38.

The court then provided three steps that counsel should use as guidelines to promote the continued preservation of potentially relevant information:

- (1) Issue a “litigation hold” at the outset of litigation or whenever litigation is reasonably anticipated. The hold should be periodically re-issued to alert new employees and to refresh the memories of current employees.
- (2) Communicate the preservation duty clearly and directly to the “key players” in the litigation (i.e. those identified in the opposing party’s initial disclosure and any subsequent supplementation thereto).
- (3) Instruct all employees to produce electronic copies of the relevant files, and ensure that all backup media that must be retained is identified

ELECTRONIC DISCOVERY

and stored in a safe place. If only a small number of backup tapes are involved, counsel might even take physical possession of them. In larger cases, perhaps counsel should segregate relevant tapes and place them in storage. At bottom, the point is to cull the relevant backup tapes from the others in order to eliminate the possibility that the tapes will be inadvertently recycled.

Id. at *39-*41.

These guidelines suggest that counsel must approach its duty to preserve holistically, appreciating that the client may need thorough and ongoing instruction about how to properly safeguard relevant electronic information.

D. What Must be Preserved?

A party that has come under a duty to preserve electronic information must also face the complicated question of what exactly must be preserved. As the note to proposed Federal Rule 26(f) points out, the volume and dynamic nature of electronically stored information may complicate preservation obligations. Even ordinary use of computers involves both the automatic creation and automatic deletion or overwriting of information. Protecting a business from a potential spoliation accusation therefore involves striking a balance between appropriate destruction of stale documents (document retention) and adequate safeguarding of documents that may be relevant to litigation (document preservation).

ELECTRONIC DISCOVERY

It used to be rather straightforward for counsel to safeguard adequately documents potentially relevant to pending (or foreseeable) litigation. Counsel needed only to cull the client's file cabinets for important documents and to inform the client that those documents were not to be shredded until they resolved the dispute.

In disputes involving large organizations, it might be necessary to suspend the company's document-destruction policy with regard to potentially discoverable documents. Having culled the files and suspended the document-destruction policy, the relevant documents were in all likelihood preserved. All that was left to be done was to review those documents and identify those that are discoverable in litigation.

In the age of electronic discovery, however, counsel must be proactive. This is so because electronic files evolve every time a computer is turned on, which causes electronic files to be inadvertently altered or destroyed by simply maintaining the status quo. Further, many organizations employ "auto-delete" programs, which systematically delete e-mail after a prescribed period of time. Individuals within the organization may inadvertently delete potentially relevant information. Finally, backup tapes—which are often recycled—may contain relevant information that would be lost if proactive steps are not taken. Thus, when it comes to electronic data, parties involved in litigation must take immediate steps to ensure that potentially relevant electronic data is not lost. Some suggested steps are detailed below.

ELECTRONIC DISCOVERY

Guidance from commentators provides practical strategies for dealing with electronic discovery. When a business has systematic procedures for retaining important files and discarding stale files, they are more likely to be prepared to preserve evidence when litigation or an investigation looms.¹⁶

Most businesses employ a backup-tape procedure to preserve their organizational data for purposes of disaster recovery. But most businesses automatize the process, and it can be difficult to quickly suspend automatic document destruction. Litigation should therefore prompt an attorney to notify its client to evaluate its retention policies or to notify its opponents, potential opponents and third parties of their duty to preserve evidence. Moreover, a party under a duty to preserve should engage its Information Technology team to ensure that the business or organization:

- (1) halts all document destruction policies, including any policies to halt recycling of backup tapes;
- (2) stops any automatic destruction protocols or system maintenance such as defragmentation;
- (3) does not install any new software that might overwrite relevant data;

16. See Lange, Michele C. S. and Kristin M. Nimsger, Electronic Evidence and Discovery: What Every Lawyer Should Know, 52-64 (2004) (providing detailed advice for document retention policies).

ELECTRONIC DISCOVERY

(4) ensures that virus protection software and techniques are up to date and properly working;

(5) preserves website content and links;

(6) creates a bit by bit copy of any potentially relevant hard drives; and

(7) notifies all persons with knowledge of relevant facts to preserve relevant information.¹⁷

These are but a few of the steps cautious counsel will take.¹⁸

Other suggestions abound: An attorney who represents a party who will seek electronic discovery should also send a “preservation letter” to put their opponent on notice and to identify as specifically as possible the types of information they should preserve and the possible places that information may

17. *See* Gates Rubber Co. v. Bando Chem. Ind., 167 F.R.D. 90 (D. Colo. 1996).

18. The suggestions in this list and others can be found in Lange, *supra* note 16, at 52-64.

ELECTRONIC DISCOVERY

exist.¹⁹ Similarly, the Manual for Complex Litigation suggests that courts should consider whether to issue a “preservation order” to define the scope of their duty to preserve electronic records.²⁰ Pursuant to a motion for such an order, parties could suggest date ranges, lists of individual electronic documents, custodians, and keywords to narrow the duty to preserve. Additionally, the parties may seek stipulations regarding the scope of their respective document retention duties.²¹ Finally, the early stages of litigation are an excellent time to consider appointing a third-party neutral electronic evidence expert who can help the parties define a mutual protocol for the various aspects of discovering electronic data.²²

Obviously, steps to comply with these suggestions could quickly cripple a party’s operations. Mercifully, the Civil Rules Advisory Committee for the proposed federal rules recognizes that an overbroad approach to preservation may be prohibitively expensive and unduly burdensome for parties dependant on their computer systems for operations. Proposed Rule 26(f) adds language that directs the parties to discuss any issues relating to preservation of discoverable

19. Joan E. Feldman & Rodger I. Kohn, *Collecting Computer-Based Evidence*, N.Y.L.J. (January 26, 1998), available at <www.law.com/ny/tech/012698t6.html>.

20. MANUAL FOR COMPLEX LITIGATION (THIRD) § 21.422, at 75 (Federal Judicial Center 1999).

21. *See* Lange, *supra* note 16, at 67.

22. *See* Lange, *supra* note 16, at 67.

ELECTRONIC DISCOVERY

information during their conference to develop the discovery plan. The parties are to be specific, balancing preservation needs with the need to continue ordinary operations of their computer systems. Proposed Rule 16(b)(5) states that the scheduling order should include provisions relating to discovery of electronic information that emerge from the parties' conference and that the court approves, which may include preservation of electronic information.

E. How Should Information Be Preserved?

What might surprise most practitioners is that the mere act of booting a computer may damage critical evidence and may change the data. Further, booting the system may overwrite the startup data on the hard drive that would have remained more accessible if the boot had not occurred.²³ Safeguarding data from inadvertent alteration involves two steps: Collecting the data and imaging the originals.

Both of these steps will likely require a computer forensics expert. This is because any failure to adhere strictly to industry standards could possibly result in lost data and may also taint the reliability of any data that is recovered, risking that a court would render it inadmissible. An expert's familiarity with the most sophisticated techniques and standards underscores why a computer forensics expert plays a vital role in the data collection process. Further, a computer forensics expert can retrieve data from nearly any location, including damaged or antiquated systems.

23. See Lange, *supra* at note 16.

ELECTRONIC DISCOVERY

Once relevant data is retrieved, the forensics expert should “mirror-image” the data in order to leave the original in tact while the expert works with an exact duplicate of the original. Indeed, it is best to make two images—saving one copy for archival purposes and using the other copy for investigation. Best practices require a complete bit-by-bit image of the data, which can be performed without even turning the computer on, thereby preserving the evidentiary value of an operating system that is identified as relevant.

III. PRODUCTION

Any good discussion of what must be produced begins with definitions of the different types of data. Data can be broadly divided into two categories: active data and residual data. Active data is information that resides on the user’s hard drive and/or network server and is readily accessible to computer users through file manager programs. By contrast, residual data is comprised of deleted files and e-mail to which the reference has been removed from the directory listings and file allocation table. This data is usually recoverable until it is overwritten by another file.

The distinction between active and residual data is important because the discovery rules treat these types of data differently. There is no question that active files must be produced. Residual data, on the other hand, raises arguments about whether residual files are in the party’s possession. One could certainly argue that, having been deleted, these files are analogous to documents already shredded or discarded in the trash. Since courts do not require parties to retrieve

ELECTRONIC DISCOVERY

destroyed or discarded paper documents, why should deleted electronic documents be treated any differently?

A. What Must Be Produced?

At least one court has taken the view that deleted electronic data should be treated no differently than paper that has been thrown away. In *Rowe Entm't, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421 (S.D.N.Y. 2002), the court discussed whether a defendant would be compelled to retrieve deleted e-mail messages. The court distinguished between currently accessible data that a party expects to be able to access for business purposes with vestigial data that is not retained for business purposes, but only for backup purposes in the case of an emergency or simply because it has neglected to discard it. *Id.* at 430-31. The former type of data must be produced, while it is unwarranted for a defendant to produce the latter at its own expense. *Id.*

The court observed that the same rationale holds force with e-mails which, although deleted from the user's active files, remain on the hard drive.

Aside from the occasional practice of "dumpster diving," the discovery of deleted computer documents does not have a close analogue in conventional, paper-based discovery. Just as a party would not be required to sort through its trash to resurrect discarded paper documents, so it should not be obligated to pay the cost of retrieving deleted e-mails.

ELECTRONIC DISCOVERY

Id. at 431. Since plaintiffs had not shown that this defendant accessed its backup tapes or deleted e-mail messages in the normal course of its business, the sought-after information did not qualify as active data, and the court declined to compel defendant to retrieve the deleted e-mail messages. *Id.*

Many courts, however, have declined to view deleted messages as analogous to thrown-away paper since deleted messages can be retrieved, albeit at considerable expense. *See* Part III.E (discussing these cases in the context of cost-shifting analysis). And even a court not ordinarily inclined to order a party to produce deleted data may do so in the face of evidence that the party deleted data in bad faith or without regard to current litigation. In *Playboy Enters., Inc. v. Welles*, 60 F. Supp. 2d 1050 (S.D. Ca. 1999), the defendant admitted that e-mail messages were deleted routinely in the ordinary course of business after the lawsuit was filed. The court ordered defendant to permit plaintiff to access the hard drive to recover the deleted messages. *Id.* at 1058.

Thus, a prophylactic rule: if evidence relevant to current or foreseeable litigation resides in deleted form on the hard drive, it is best to preserve it. It is reasonable to expect that residual data must be produced since it can often be recovered.

B. How Does a Party Produce Information that is “Not Reasonably Accessible?”

The proposed amendments to Federal Rule 26(b)(2) state that a party need not provide discovery of electronically stored information that is not reasonably

ELECTRONIC DISCOVERY

accessible unless the court orders discovery for good cause. If the requesting party moves to compel discovery under Rule 37(a), the responding party must show that the information is not reasonably accessible. The Committee Note to the Rule 26(b)(2) seeks to clarify what “reasonably accessible” means, describing what will likely be a case-by-case definition:

Whether given information is “reasonably accessible” may depend on a variety of circumstances. One referent would be whether the party itself routinely accesses or uses the information. If the party routinely uses the information—sometimes called “active data”—the information would ordinarily be considered reasonably accessible. The fact that the party does not routinely access the information does not necessarily mean that access requires substantial effort or cost.

There is another reason that “reasonably accessible” is an evolving definition. The very problems created by the advent of electronic data may also be solved by electronic means. As technology progresses, we can only hope that it will remove some of the obstacles to producing electronically stored information.

The Civil Rules Advisory Committee also clarifies the process by which the parties handle assertions that information is not reasonably accessible: Assuming a party has reason to believe requested information is not “reasonably accessible,” it must then identify the information it is neither reviewing nor

ELECTRONIC DISCOVERY

producing on this ground. The responding party may be more or less specific, so long as it informs the other party that information has been withheld on this basis, the nature of the information withheld, and the basis for believing the information is not reasonably accessible. For example, a responding party may describe information categorically, such as all information stored solely for disaster-recovery purposes. If the responding party has actually accessed the requested information, it foregoes any reliance on this rule as a basis for withholding information.

The requesting party may move to compel discovery, thereby requiring the responding party to show that the information sought is not reasonably accessible. It is then up to the court to determine whether the information is reasonably accessible *vel non* and to consider appropriate conditions on production. Such conditions might include:

- sampling electronically stored information to gauge the likelihood that relevant information would be obtained;
- weighing the importance of that information in light of the burdens and costs of production;
- limiting the amount of information to be produced; and
- implementing provisions regarding cost of production.

ELECTRONIC DISCOVERY

Through this interplay between the parties and the court, it is clear that the Committee intends for a responding party to have some protection from potentially burdensome discovery requests.

C. In What Form Must Information be Produced?

In contrast to conventional discovery, in which paper can only be produced as paper, electronic discovery presents various options. Information can be produced not only in paper or electronic form, but in different electronic formats. The proposed amendments to Federal Rules 16(b) and 26(f)(3) and to Form 35 direct the parties to consider, and the court to include in the scheduling order, provisions for discovery of electronically stored information.

Additionally, the proposed changes to Rules 33 and 34 now contemplate the differences between producing documents and producing electronically stored information. The proposed amendments to Rule 33 provide that when a party answers an interrogatory involving review of business records, it should also search electronically stored information and permit the responding party to answer by providing access to that information. Rule 33(d) allows a responding party to substitute access to electronically stored information for an answer in cases where the burden of delivering the answer will be substantially the same for either party. Should the responding party elect this option, it must ensure that the interrogating party is able to locate and identify the information as readily as the responding party, and the responding party must give the interrogating party a “reasonable opportunity to examine, audit or inspect” the information.

ELECTRONIC DISCOVERY

The proposed amendments to Rule 34 account for the ambiguity and limitations of the word “documents” by specifically adding “electronically stored information.”²⁴ This distinction means that lawyers should frame discovery requests to specify whether they seek discovery of documents, electronically stored information, or both.

Furthermore, the proposed amendments to Federal Rule 34(b) authorize the requesting party to specify the form in which electronically stored information should be produced²⁵ and set up a framework for resolving disputes over the form of producing such information. If the interrogating party does not request that electronically stored information be produced in a specific form, and in the absence of party agreement or court order as to form, the producing party has two options: (1) to produce information in a form in which it is ordinarily maintained, or (2) to produce information in an electronically searchable form.²⁶ As the

24. *See, e.g.,* Crown Life Ins. Co. v. Craig, 995 F.2d 1376 (7th Cir. 1993) (upholding sanctions against a party that failed to produce electronic data on the grounds that information in the database was not in “document” form, and holding that “document” includes computer data).

25. Texas Rule of Civil Procedure 196.4 already addresses this issue. It provides that parties must specifically request electronic data where it is desired and must designate the form in which it is to be produced.

26. *See, e.g.,* Sattar v. Motorola, Inc., 138 F.3d 1164 (7th Cir. 1997) (ordering defendant to equip plaintiff with the means to read its e-mail files or pay half the

ELECTRONIC DISCOVERY

Committee Note to the Rule points out, these choices are analogous to the choices presented when producing paper documents: the form in which they are kept in the usual course of business or organized and labeled to correspond to the categories in the request.

Two other clarifications in the proposed rule are useful: One, absent court order or party agreement, the responding party need only produce the information in one form. Also, the obligation to produce for testing and sampling applies to electronically stored information and documents, as well as tangible things and land or other property.^{27, 28}

D. Issues that Arise with Production of Electronic Evidence

As with traditional discovery, electronic discovery presents challenges for counsel, who must screen for privileged or private information before producing it.

costs of production when it produced tapes on four-inch tapes that plaintiff was unable to read).

27. *See also* Playboy Enters., Inc. v. Welles, 60 F. Supp. 1050, 1052-53 (S.D. Cal. 1999) (ordering Welles to make her computer hard drive available for inspection, as Rule 34 contemplates access to data compilations).

28. *Cf.* TEX. R. CIV. P. 196.6.

ELECTRONIC DISCOVERY

1. Privilege Review and Waiver

Perhaps the most problematic issues related to production of electronic evidence are privilege review and waiver. When information is stored electronically, it compounds the burden, costs, and difficulties of privilege review. Materials subject to a claim of privilege can be more difficult to identify, in part because of metadata (automatically created identifying information) and embedded data (earlier edits that would not appear on a paper view or the computer monitor image).

Parties can minimize the burden of an exhaustive privilege review by agreeing to protocols that minimize the risk of waiver. These protocols might include “quick peek” or “claw back” arrangements, such as that provided for in Texas Rule of Civil Procedure 193.3(d). Best practices recommendations promulgated by The Sedona Conference also suggest that courts should consider entering protective orders protecting the parties from waiving their privileges:

Because of the large volumes of documents and data typically at issue in cases involving production of electronic data, courts should consider entering orders protecting the parties against any waiver of privileges or protections due to the inadvertent production of documents and data. . . .

Such an order should provide that the inadvertent disclosure of a privileged document does not constitute a waiver of privilege, that the privileged document should be returned (or there will be a certification that it has been deleted), and that any notes or copies will be destroyed or

ELECTRONIC DISCOVERY

deleted. Ideally, an agreement or order should be obtained prior to any production.²⁹

The Manual for Complex Litigation also notes the onerous burden associated with privilege review and waiver and suggests the parties stipulate to a “nonwaiver” agreement:

A responding party’s screening of vast quantities of unorganized computer data for privilege prior to production can be particularly onerous in those jurisdictions in which inadvertent production of privileged data may constitute a waiver of privilege as to a particular item of information, items related to the relevant issue, or the entire data collection. Fear of the consequences of inadvertent waiver may add cost and delay to the discovery process for all parties. Thus, judges often encourage counsel to stipulate to a “nonwaiver” agreement, which they can adopt as a case-management order. Such agreements protect the responding parties from the most dire consequences of inadvertent waiver by allowing them to

29. *See* The Sedona Conference, *The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production* (March 2003), comment 10a, available at <www.thesedonaconference.org/publications_html>.

ELECTRONIC DISCOVERY

“take back” inadvertently produced privileged materials if discovered within a reasonable period, perhaps thirty days from production.

THE MANUAL FOR COMPLEX LITIGATION (4th) § 11.446.

Although the proposed amendments to the federal rules do not require parties to reach these sorts of agreements, they do facilitate the process. The proposed amendments to Rule 16(b)(6), Rule 26(f)(4), and Form 35 provide that if the parties can agree to an arrangement that allows production without a complete privilege review and protects against waiver, the court may enter a case-management order adopting the agreement.^{30,31}

2. Privacy Concerns

Privacy concerns are also an issue with electronic discovery. What happens, for example, when the opposing party requests an entire database or seeks to image an entire hard drive, which would reveal what web sites have been visited and any other privately stored information? While there is no clear holding on this issue, the Texas Supreme Court has intimated that the broad scope of discovery must sometimes be narrowed to account for privacy concerns.

30. Of course, parties may make such agreements even when dealing only with paper discovery. The privilege stipulations are particularly practical, however, when dealing with voluminous information stored electronically.

31. Practical suggestions for managing voluminous data are discussed, *infra*, with the cost-shifting tests in Part III.E.

ELECTRONIC DISCOVERY

In *In re Ci Host, Inc. v. Creative Innovations, Inc.*, 92 S.W.3d 514, (2002), the Texas Supreme Court considered a trial court order to produce all backup tapes, even though some tapes contained protected information and e-mails that may be considered confidential by some of the business's customers. Although the business had waived its objections to the discovery request, the court maintained that it was "loath to allow [the business] to unilaterally waive its customers' privacy rights by its failing to adhere to the discovery rules." *Id.* at 517 (citing *Eli Lilly & Co. v. Marshall*, 850 S.W.2d 155, 160 (Tex. 1993)). It therefore denied a writ of mandamus to order production in order to allow the trial court and parties to address the privacy considerations.

In *Eli Lilly*, the Texas Supreme Court balanced the broad discovery rules against the "compelling public interest considerations" manifested by FDA privacy regulations. 850 S.W.2d at 160. The court recognized that, under the doctrine of shared discovery, the fruits of discovery are available not only to parties but also to other litigants and potential litigants. *Garcia v. Peeples*, 734 S.W.2d 343, 347 (Tex. 1987). But the opposing party may have a legitimate interest in avoiding discovery based on a "compelling, particularized interest in nondisclosure." *Eli Lilly*, 850 S.W.2d at 160. In such cases, the court holds that it may be an abuse of discretion to order disclosure that would reveal confidential information absent a showing of particularized relevance and need.

As these cases show, electronic discovery may often require creative problem solving and good communication with opposing counsel about the unique needs and issues of the case. Counsel would do well to address ways to

ELECTRONIC DISCOVERY

prevent waiving privilege and to account for privacy concerns early in the discovery process.

E. Who Must Bear the Costs of Producing Electronic Information?

The final area that complicates production of electronically stored information is the issue of cost shifting. Under the discovery rules, it is presumed that the responding party must bear the expense of complying with discovery requests. *Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 358 (1978).

Discovery rules, such as Federal Rules of Civil Procedure 34 and 26 and Texas Rule of Civil Procedure 192.7(b), limit the universe of material that the producing party must generate to things that are in its possession, custody, or control in the ordinary course of business. Because producing parties cannot be compelled to bear the cost of producing material outside their “possession,” many litigators have argued that electronic files that are deleted, archived, or not reasonably accessible are not within their “possession” and should not have to be produced.

But courts that have considered these arguments are generally unsympathetic. In *Delozier v. First Nat’l Bank of Gatlinburg*, 109 F.R.D. 161 (E.D. Tenn. 1986), the court stated, “[a] court will not shift the burden of discovery onto the discovering party where the costliness of the discovery procedure involved is entirely a product of the defendant’s record-keeping scheme over which the plaintiff has no control.” If a party chooses to maintain records in a format that cannot be easily accessed, that party will also have to bear the

ELECTRONIC DISCOVERY

financial consequences when it must produce any potentially relevant material therein. *See, e.g., In re Brand Name Prescription Drugs Antitrust Litig.*, 1995 WL 360526 (N.D. Ill. June 15, 1995) (requiring defendant to produce responsive e-mail at its own expense where the high costs of retrieving the data was mainly due to its own record-keeping scheme).

A court may nevertheless protect the responding party from “undue burden and expense” by shifting some or all of the costs of production to the requesting party. *Oppenheimer*, 437 U.S. at 358. (citing Fed. R. Civ. P. 26(c)). In *Oppenheimer*, the U.S. Supreme Court wrote, “We do not think a defendant should be penalized for not maintaining his records in the form most convenient to some potential future litigants whose identity and perceived needs could not have been anticipated.” *Id.* at 363. Because the expense of creating computer programs that would locate the requested data was the same for either party, the Court ultimately ordered the requesting party to bear the cost of production.

More recently, in *Zonaras v. General Motors Corp.*, 1996 WL 1671236 (S.D. Ohio Oct. 17, 1996), the court held that, because the requested evidence was not necessarily admissible, the requesting party should pay half of the production costs incurred by the producing party. This type of reasoning focuses on the utility of the evidence and the effort and expense involved in obtaining it—a burden versus benefit analysis.³² This analysis is reflected in Texas Rule of Civil Procedure 196.4. The Texas Rule provides that the responding party must produce responsive electronic data that is reasonably available to the responding

32. *See Lange, supra* note 16, at 72.

ELECTRONIC DISCOVERY

party in the ordinary course of business. But if the responding party cannot—through reasonable efforts—retrieve or produce the requested information, it may object. The court may then order the responding party to comply with the request, but it must also order that the requesting party pay the reasonable expenses of any extraordinary steps required to retrieve and produce the information.

The most recent cost-shifting decisions rely on a more formal, multi-factored approach created by courts in the Southern District of New York. There are two significant tests: an eight-factor test set forth in *Rowe* and a seven-factor test modifying *Rowe* set forth in the *Zubulake* opinions. See *Rowe Entertainment, Inc. v. The William Morris Agency*, 205 F.R.D. 421 (S.D.N.Y. 2002); *Zubulake v. Warburg*, 217 F.R.D. 309 (S.D.N.Y. 2003) (“*Zubulake I*”).

The *Rowe* court began with the premise that the traditional rule that the producing party bears the cost of discovery does not necessarily prevail in the electronic discovery context. Instead:

even if this principle is unassailable in the context of paper records, it does not translate well into the realm of electronic data. The underlying assumption is that the party retaining information does so because that information is useful to it, as demonstrated by the fact that it is willing to bear the costs of retention. That party may therefore be expected to locate specific data, whether for its own needs or in response to a discovery request. With electronic media, however, the syllogism breaks down because the costs of storage are virtually nil. Information is retained not

ELECTRONIC DISCOVERY

because it is expected to be used, but because there is no compelling reason to discard it. And, even if data is retained for limited purposes, it is not necessarily amenable to discovery.

Id. at 429.

The *Rowe* court then used the following eight factors to determine who should pay the costs of production:

(1) the specificity of the discovery requests (the less specific, the more appropriate it is to shift costs);

(2) the likelihood of discovering critical information (the more likely it is that critical information will be found, the more fair it is to force a producing party to pay);

(3) the availability of such information from other sources (if equivalent information is available from another source, the requesting party should pay for the electronic production);

(4) the purposes for which the responding party maintains the requested data (if a party maintains data for use in current activities, it is fair to make them pay for its production in litigation);

ELECTRONIC DISCOVERY

(5) the relative benefit to the parties of obtaining the information (where the responding party benefits from the production, there is less rationale to shift costs);

(6) the total cost associated with production (if the total cost of the requested discovery is not substantial, there is no cause to deviate from the presumption that the responding party will bear the expense);

(7) the relative ability of each party to control costs and its incentive to do so (where the discovery process is going to be incremental, it is more efficient to place the burden on the party who will decide how expansive the discovery will be); and

(8) the resources available to each party (the ability of each party to bear the costs of discovery may be an appropriate consideration).

Rowe Entertainment, Inc., 205 F.R.D. at 429-32.

This test quickly became recognized as the “gold standard” for courts resolving electronic discovery cost-allocation disputes.³³ Thus the parties in

33. James M. Evangelista, *Polishing the “Gold Standard” on the E-Discovery Cost-Shifting Analysis: Zubulake v. UBS Warburg, LLC*, 9 J. TECH. L. & POL’Y 1 (2004).

ELECTRONIC DISCOVERY

Zubulake naturally assumed this would be the test the court would apply to determine whether cost-shifting was appropriate. Instead, Judge Scheindlin saw a need to ameliorate the eight-factor test to cure an apparent imbalance in the decisions that followed *Rowe*. Judge Scheindlin observed that “of the handful of reported opinions that apply *Rowe* or some modification thereof, all of them have ordered the cost of discovery to be shifted to the requesting party.” *Zubulake*, 217 F.R.D. at 320. Judge Scheindlin therefore decided that “in order to maintain the presumption that the responding party pays, the cost-shifting analysis must be neutral; close calls should be resolved in favor of the presumption.” *Id.*

Modifying the *Rowe* test into a new, seven-factor test, Judge Scheindlin eliminated one of the *Rowe* factors, combined two *Rowe* factors, and added a new factor:

- (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;

ELECTRONIC DISCOVERY

(5) the relative ability of each party to control costs and its incentive to do so;

(6) the importance of the issue at stake in the litigation; and

(7) the relative benefits to the parties of obtaining the information.

Id. at 322.

Judge Scheindlin also provided some guidance for applying the test. She emphasized that despite the temptation to treat the factors as a checklist, “we do not just add up the factors.” *Id.* Instead, the central question must be, does the request impose an “undue burden or expense” on the responding party, i.e., “how important is the sought-after evidence in comparison to the cost of production?” *Id.* at 322-23. Thus, the factors are weighed in descending order of importance, with extra emphasis on the first two factors. *Id.* at 323.

The *Zubulake* test provides the most practical guidance of any test to date. It may be fair to say that it is the current “gold standard” for determining whether it is appropriate to shift costs to the requesting party.

Although *Zubulake* may be considered the “gold standard,” practitioners should note that it has not yet been adopted by a Texas court. In fact, the only court to consider the opinion has distinguished the facts, noting that *Zubulake* is not binding authority in Texas. *Multitechnology Servs., L.P. v. Verizon Southwest*, 2004 U.S. Dist. LEXIS 12957 (N.D. Tex. July 12, 2004). Nor do the

ELECTRONIC DISCOVERY

Texas Rules provide any guidance on this issue. However, the Texas Supreme Court Advisory Committee acknowledges the need for consistency among the federal and state courts—especially in regards to electronic discovery issues. It therefore plans to examine the current Texas rules and determine whether any changes are necessary in light of the proposed Federal rules.

Before leaving this topic, it is imperative to note that an undue burden or expense does not arise just because electronic evidence is involved. Electronic evidence is frequently cheaper and easier to produce than paper evidence because it can be searched automatically, key words can be run for privilege checks, and the production can be made in electronic form, obviating the need for mass photocopying.³⁴ Indeed, the plaintiffs in *Rowe* identified a number of ways that defendants could minimize the cost of responding to the request, including:

- (1) identify key personnel rather than retrieving the e-mail of all employees;
- (2) restore only a portion of archival tapes, based on date restrictions and sampling;
- (3) produce e-mail in electronic rather than paper form; and

34. See Evangelista, *supra* note 33.

ELECTRONIC DISCOVERY

(4) conduct automatic searches for privilege and responsiveness by using key words, rather than by using a detailed human review.

Rowe, 205 F.R.D. at 427. Thus, the *Zubulake* test is only appropriate in those cases where an electronic discovery request really imposes an extraordinary cost and burden. In other cases, the parties may just find that technology is their friend, a tool that can be used to tame itself.

IV. SANCTIONS

Texas trial courts have broad power to police litigants and protect against evidence spoliation. Texas Rule of Civil Procedure 215(3) allows trial courts to sanction a party whenever it abuses the discovery process. Where Rule 215 may not apply—such as when a party destroys evidence before suit is filed—a trial court has inherent power to remedy spoliation. *Eichelberger v. Eichelberger*, 582 S.W.2d 395, 398 (Tex. 1979) (holding that trial courts have inherent judicial power to take action that will “aid in the exercise of its jurisdiction, in the administration of justice, and in the preservation of its independence and integrity”).³⁵ Accordingly, trial judges have broad discretion to take measures ranging from a jury instruction on the spoliation presumption to, in the most egregious case, death penalty sanctions. *Trevino v. Ortega*, 969 S.W.2d 950, 953

35. *Cf.* *Turner*, 142 F.R.D. at 72 (inherent power in Federal Rule 37); *Shepherd v. Am. Broadcasting Cos.*, 62 F.3d 1469, 1474 (D.C. Cir. 1995) (inherent power in federal courts).

ELECTRONIC DISCOVERY

(Tex. 1998) (citing *Watson v. Brazos Elec. Power Coop., Inc.*, 918 S.W.2d 639, 643 (Tex. App.—Waco 1996, writ denied) (holding that trial court erred when it failed to give a spoliation instruction); *Ramirez v. Otis Elevator Co.*, 837 S.W.2d 405, 412 (Tex. App.—Dallas 1992, writ denied) (noting that a trial court possesses wide discretion in awarding discovery sanctions); *see also* TEX. R. CIV. P. 215(b).

Although trial courts have broad discretion to choose an appropriate sanction, *see TransAmerican Natural Gas Corp. v. Powell*, 811 S.W.2d 913, 917 (Tex. 1991), no single remedy is appropriate for all cases. Rather the trial court must respond appropriately based upon the facts of each case, considering factors such as the degree of the spoliator's culpability and the prejudice the nonspoliator suffers. *See, e.g., San Antonio Press, Inc. v. Custom Bilt Mach.*, 852 S.W.2d 64, 67 (Tex. App.—San Antonio 1993, no writ). The court must also direct the sanction against the wrongdoer and ensure it is properly tailored to remedy the prejudice caused the innocent party.³⁶ *TransAmerican*, 811 S.W.2d at 917.

36. As the Zubulake court put it, the major consideration in choosing an appropriate sanction—along with punishing the spoliator and deterring future misconduct—is to restore the wronged party to the position that it would have been in had the spoliator faithfully discharged its discovery obligations. Zubulake IV, 2004 U.S. Dist. LEXIS at *51.

ELECTRONIC DISCOVERY

A. Death Penalty Sanctions and Excluding Evidence

In the spoliation context, courts may dismiss the case or render a default judgment against the spoliator or exclude evidence or testimony. A “death penalty” sanction—dismissal, default judgment, or striking plaintiff’s pleadings—is justified when a party destroys evidence with the intent to subvert discovery. *Trevino*, 969 S.W.2d at 959 (Baker, J., concurring) (citing *Computer Assocs. Int’l Inc. v. American Fundware*, 133 F.R.D. 166, 169 (D. Colo. 1990); *Wm T. Thompson Co.*, 593 F. Supp. at 1456. In these cases, the spoliator’s conduct was egregious, the prejudice to the nonspoliating party great, and imposing a lesser sanction would not cure the prejudice effectively. *See TransAmerican*, 811 S.W.2d at 917-18; *Remington Arms Co. v. Caldwell*, 850 S.W.2d 167, 171 (Tex. 1993). Ordinarily, a trial court would be required to test the effectiveness of lesser sanctions by actually implementing and ordering each sanction that would be appropriate to promote compliance with the trial court’s orders. *Cire v. Cummings*, 134 S.W.3d 835, 842 (Tex. 2004) (citing *Chrysler Corp. v. Blackmon*, 841 S.W.2d 844, 849 (Tex. 1992)). But when a party engages in egregious conduct and blatantly disregards the discovery process by destroying the very evidence that could prove (or disprove) its case, along with violating multiple court orders to produce the evidence, “death penalty sanctions are clearly justified.” *Cire*, 134 S.W.3d at 842.

Less severe, but nonetheless quite serious is a court’s decision to exclude evidence or testimony. Courts generally use this sanction when the spoliating

ELECTRONIC DISCOVERY

party attempts to admit testimony or evidence adduced from the destroyed evidence. *Trevino*, 969 S.W.2d at 960 (Baker, J., concurring).

B. Instructions

In addition to sanctions, Texas trial courts also have broad discretion in instructing juries. TEX. R. CIV. P. 277; *Mobil Chem. Co. v. Bell*, 517 S.W.2d 245, 256 (Tex. 1975). An adverse instruction is a common remedy for spoliation, dating back to English common law. *See Armory v. Delamirie*, 93 Eng. Rep. 664 (K.B. 1722); *Rex v. Arundel*, 80 Eng. Rep. 258 (K.B. 1617). Its purpose is captured in the Latin maxim *omnia presumuntur contra spoliatores*, “all things presumed against a despoiler or wrongdoer.” BLACK’S LAW DICTIONARY 1401 (6th ed. 1997). Texas courts have applied this presumption for over a century and have characterized it as an inference to be drawn by the jury. *Curtis & Co. Mfg. Co. v. Douglas*, 79 Tex. 167, 15 S.W. 154, 155 (Tex. 1890).

When a party is prejudiced by spoliation, the trial court can assess the severity of prejudice and submit to the jury one of two types of instructions. *See Welsh*, 844 F.2d at 1239. The more severe of the two—a rebuttable presumption—is primarily used when the nonspoliating party cannot prove its prima facie case without the destroyed evidence. *Id.* at 1248. A rebuttable presumption entails instructing the jury that the spoliating party has negligently or intentionally destroyed evidence, and the jury should therefore presume that evidence was unfavorable to the spoliating party on the particular fact or issue the destroyed evidence might have supported unless the spoliating party can disprove

ELECTRONIC DISCOVERY

that presumed fact or issue. This approach takes the middle ground of shifting the burden of proof to the culpable party while allowing it to prosecute or defend its case.

The second, less severe type of presumption is an adverse presumption. An adverse presumption merely states that the evidence would have been unfavorable to the spoliating party. *See H.E. Butt Grocery Co. v. Bruner*, 530 S.W.2d 340, 344 (Tex. Civ. App.—Waco 1975, writ dismissed by agreement). The presumption itself has probative value and may be sufficient to support the nonspoliating party's assertions, *id.*, although it does not relieve the nonspoliating party of the burden to prove each element of its case. *See DeLaughter v. Lawrence Co. Hosp.*, 601 So.2d 818, 822 (Miss. 1992).

As a general rule, the Texas courts of appeals limit the use of a spoliation instruction to two circumstances: (1) the deliberate destruction of relevant evidence and (2) the failure of a party to produce relevant evidence or to explain its non-production. *See Anderson v. Taylor Publ'g Co.*, 13 S.W.3d 56, 61 (Tex. App.—Dallas 2000, petition denied) (citing *Wal-Mart Stores, Inc. v. Middleton*, 982 S.W.2d 468, 470-71 (Tex. App.—San Antonio 1998, petition denied)). The first circumstance envisions that a party who has deliberately destroyed evidence does so because the evidence was unfavorable to its case. *See Williford Energy Co. v. Submersible Cable Servs., Inc.*, 895 S.W.2d 379, 389-90 (Tex. App.—Amarillo 1994, no writ); *Brewer v. Dowling*, 862 S.W.2d 156, 159 (Tex. App.—Fort Worth 1993, writ denied). The second circumstance raises the adverse presumption because the party controlling the missing evidence cannot explain its failure to

ELECTRONIC DISCOVERY

produce it. *See Watson v. Brazos Elec. Power Co-op., Inc.*, 918 S.W.2d 639, 643 (Tex. App.—Waco 1996, writ denied).

The following instruction, given in a suit against Wal-Mart, is a good example of what a jury might be asked to consider when evidence is lost or destroyed:

You are instructed that, when a party has possession of a piece of evidence at a time he knows or should have known it will be evidence in a controversy, and thereafter he disposes of it, makes it unavailable, or fails to produce it, there is a presumption in law that the piece of evidence, had it been produced, would have been unfavorable to the party who did not produce it. If you find by a preponderance of the evidence that Wal-Mart had possession of the reindeer at a time it knew or should have known they would be evidence in this controversy, then there is a presumption that the reindeer, if produced, would be unfavorable to Wal-Mart.

Johnson, 106 S.W.3d at 720-21. Although the court reversed the judgment against Wal-Mart because it had no duty to preserve the evidence, this type of instruction may hang like the sword of Damocles over a defendant's case.

C. MasterCard and Philip Morris—Spoliation Sanctions in Practice

Two cases help to demonstrate how trial courts impose various sanctions depending on the spoliator's level of culpability and potential damage to

ELECTRONIC DISCOVERY

plaintiff's case. In *MasterCard Int'l, Inc. v. Moulton*, 2004 WL 1393992 (S.D.N.Y. June 22, 2004), MasterCard asserted a copyright infringement claim against the operators of a pornographic Web site. Neglecting to implement a litigation hold, defendants destroyed four months' worth of documents after the litigation began. The defendants argued that no effort was made to print or save the e-mails before they were automatically destroyed by the computer server because e-mails were routinely eliminated in the ordinary course of business. Although the court was not persuaded that the documents were destroyed in bad faith, (for the express purpose of obstructing the litigation), it did emphasize that the absence of bad faith does not protect a party from appropriate sanctions. *Id.* at *4. Since a specific intent to thwart litigation is not required, even simple negligence is a sufficiently culpable state of mind to justify a spoliation finding.³⁷ The court therefore granted plaintiff's request for an adverse inference instruction, reasoning that "the very fact that the e-mails are missing leaves us in the realm of speculation as to what they contained and in what manner they might have assisted plaintiff in litigating its claims. *Id.* at *5.

Similarly, the United States District Court for the District of Columbia considered appropriate sanctions for defendant's document destruction in *United States v. Philip Morris USA Inc.*, 327 F. Supp. 2d 21 (D.D.C. 2004). Several years into the government's suit for smoking and health-related issues, it discovered that Philip Morris had systematically ignored Court Order #1, requiring Philip Morris to preserve any documents potentially relevant to the

³⁷. See *Residential Funding Corp. v. DeGeorge Funding Corp.*, 306 F.3d 99, 108 (2d Cir. 2002); *Reilly v. Natwest Markets Group, Inc.*, 181 F.3d 253, 267 (2d Cir. 1999).

ELECTRONIC DISCOVERY

litigation. Defendants had continued to delete email when it became sixty days old, on a monthly system-wide basis for a period of two years after the court order was in place. Even after learning that their document retention policy was inadequate, defendants continued to destroy documents for several months, including relevant emails from at least eleven company supervisors and officers. Defendants then waited several more months to notify the court and the government about the situation. Finding that a significant number of emails had been permanently destroyed, the court declared that “it is astounding that employees at the highest corporate level in Philip Morris, with significant responsibilities pertaining to issues in this lawsuit, failed to follow [the] Order . . . which, if followed, would have ensured the preservation of those emails which have been irretrievably lost.” The court also emphasized that the employees were at the highest corporate level of a “particularly sophisticated corporate litigant which has been involved in hundreds, and more likely thousands, of smoking related lawsuits.” *Id.* at 25.

Although the court refused the government’s request for an adverse inference instruction, it granted its requests for other forms of sanctions. The court barred a key employee, as well as any other individual who failed to comply with Phillip Morris’ own internal document retention program, from testifying in any capacity at trial. *Id.* at 25. The court also ordered Philip Morris to reimburse the government for its costs and assessed \$2.75 million in sanctions. Additionally it imposed \$250,000 in sanctions on each of the eleven employees who failed to comply with the “print and retain” policy.

ELECTRONIC DISCOVERY

These cases demonstrate that courts have little tolerance for litigants' failure to preserve documents once a duty to preserve has attached. Even when a spoliator is merely negligent, sanctions are still appropriate in order to temper the "realm of speculation" that now clouds a plaintiff's case. And when the spoliator is more culpable, courts may impose more draconian measures in order to secure future compliance and to punish knowing or willful spoliation.

D. The Federal Rules Propose a Safe Harbor

The proposed amendment to Federal Rule 37 provides a narrow "safe harbor" for parties concerned about the automatic recycling, overwriting, and alteration of electronically stored information: it protects a party from sanctions under the Civil Rules for failing to provide electronically stored information lost because of the routine operation of the party's computer system. Naturally, this does not apply 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.

To invoke this "safe harbor," proposed rule 37(f) requires a party to have taken reasonable steps—what is often called a "litigation hold"—to preserve electronically stored information when the party knew or should have known it was discoverable in the action. According to the Committee Note, in most instances, a party acts reasonably by identifying and preserving reasonably accessible electronically stored information that is discoverable without court order. Obvious candidates for preservation are reasonably accessible e-mail

ELECTRONIC DISCOVERY

records and electronic files of key individuals and departments implicated by the pleadings. Yet even more caution may be required where a party knew or should have known that information was discoverable and could not be obtained elsewhere. In such cases, a party may not act reasonably unless it preserves electronically stored information that is not reasonably accessible. The proposed rules thus recognize that where a party acts reasonably, the unique issues related to preservation of electronic information should not automatically subject a party to sanctions.

V. CONCLUSION

Easy answers to electronic discovery issues are elusive. Yet this area of law is not without an increasing array of sources of guidance. Suggestions from commentators abound, case law is progressing, and proposed federal rule amendments have arrived, revealing a practical and perceptive approach to challenges that are unique to electronic discovery.

All of the guidance reduces to a single point: Counsel must take a proactive role in staying abreast of electronic discovery law, in educating and monitoring their clients when a duty to preserve evidence arises, and in understanding the unique challenges and opportunities that are presented by a case that involves electronic discovery.