Negotiating the Minefields of Electronic Discovery

Stephen D. Williger, Esq.[*] *& Robin M. Wilson, Esq.*[**]

Cite as: Stephen D. Williger & Robin M. Wilson, *Negotiating the Minefields of Electronic Discovery*, 10 RICH. J.L. & TECH. 52 (2004), *at* http://law.richmond.edu/jolt/v10i5/article52.pdf.

I. INTRODUCTION

[1] A company's employee has sued for sexual harassment, age discrimination, or wrongful termination. Or, as another example, the company has been sued for infringement of intellectual property, breach of contract, fraud, or any number of other business reasons. During the course of discovery, the plaintiff serves discovery requests, including a request for data that has been deleted from the company's electronic records but may still be contained within the company's backup systems. The search for this data is time consuming and expensive. Discoverable materials may be found in the company's backup system, but does that possibility justify the lost productivity and expense to restore the material?

[2] This common scenario calls for a considered and thorough multi-step response to ensure that a responding party fulfills all of its obligations. In particular, a responding party must address issues relating to the preservation and collection of electronic information, reviewing what are often massive quantities of potentially responsive electronic information, and determining in what form and format the responsive information will be produced. Inherent to each facet of this process is the potential cost,

[*] Stephen D. Williger is a partner in the Business Litigation practice group at the Cleveland, Ohio office of Thompson Hine LLP. He focuses his practice on business litigation, including complex fraud and securities cases.

[**] Robin M. Wilson is an associate in the Business Litigation and Product Liability practice groups at the Cleveland, Ohio office of Thompson Hine LLP. She focuses her practice on business and commercial contract disputes, governmental land use matters, and product liability litigation.

which often may exceed the generally predictable costs of traditional document discovery.

[3] How can a company safeguard its employees' time and the company's money against an onerous electronic discovery request? Who must pay the cost? How does one convince a judge that such a search is not justified? How does a company prepare so it has the systems in place and the protocols established to enable it to properly respond to electronic discovery requests in the most cost and time efficient manner?

[4] While many companies have document retention policies and procedures, those policies and procedures may well require reconsideration to account for electronic documents and the realities of their use in litigation. Because electronic discovery is playing a greater role in commercial litigation, it is important that companies develop and implement a system to address these challenges to avoid facing them for the first time during litigation.

[5] Given the vast amount of information that likely exists in electronic form, it is important for a company to have a detailed understanding of the processes necessary to respond to discovery requests seeking such information. This article sets forth the processes that are necessary in order to respond to discovery in the electronic age and frames the discussion from the perspective of a party responding to discovery requests. However, each of the issues addressed is equally important from the perspective of a requesting party.

II. ELECTRONIC INFORMATION IN THE CORPORATE SETTING

A. *Responding to a Request for Production of Electronic Information Can Be Complicated.*

[6] As the use of computers and data processing systems has increased, the scope of information potentially subject to discovery has skyrocketed. A recent study by the University of California at Berkeley's School of Information Management and Systems estimated that almost five exabytes[1] of new information were produced in 2002.[2] Of that

[1] An "exabyte" is a measure of the capacity of digital storage media that is greater than one quadrillion bytes of information. More precisely, an exabyte is comprised of 2^{60} – or 1,152,921,504,606,846,976 – bytes. To illustrate this scale, one exabyte is equal to:

information, which is roughly equal to 500,000 new libraries the size of the Library of Congress,[3] only 0.01 percent was stored in paper records, whereas nearly 92 percent of the information created was stored on magnetic media such as computer hard disks, magnetic tape, and the like.[4]

[7] Given this vast amount of information, it can fairly be assumed that nearly every legal entity subject to the jurisdiction of the state and federal courts generates and maintains at least some of its information in an electronic form. In recognition of the need to include such information within the scope of the rules governing discovery, Rule 34 of the Federal Rules of Civil Procedure was amended in 1970 to provide that, upon request, a party is required to produce "any designated documents," including "writings, drawings, graphs, charts, photographs, phonorecords, *and other data compilations* from which information can be obtained . . . ."[5]

[8] Several states have gone further by adopting rules that expressly cover discovery of electronically-stored information and the challenges inherent

---

1,125,899,906,842,624 kilobytes; 1,099,511,627,776 megabytes; 1,073,741,824 gigabytes; 1,048,576 terabytes; or 1,024 petabytes. Peter Lyman and Hal R. Varian, Executive Summary, *How Much Information*, *2003*, *at* http://www.sims.berkeley.edu/research/projects/how-much-info-2003/execsum.htm#summmary (last visited Feb. 6, 2004).

[2] Lyman & Varian, *supra* note 1.

[3] *Id*.

[4] *Id*.

[5] FED. R. CIV. P. 34 (emphasis added). The inclusion of "data compilations" as a type of information subject to production was made in the 1970 amendments to Rule 34, and was intended "to accord with changing technology." However, the advisory committee notes for FED. R. CIV. P. 34 address how information stored as electronic data is discoverable, and set forth limits to the production and protection for the respondent. It makes clear that Rule 34 applies to electronic data compilations from which information can be obtained only with the use of detection devices and that when the data can, as a practical matter, be made usable by the discovering party only through respondent's devices, respondent may be required to use its devices to translate the data into usable form. In many instances, this means that respondent will have to supply a print-out of computer data. The burden thus placed on respondent will vary from case to case, and the courts have ample power under Rule 26(c) to protect respondent against undue burden or expense, either by restricting discovery or requiring that the discovering party pay some or all costs. Similarly, if the discovering party needs to check the electronic source itself, the court may protect respondent with respect to preservation of its records, confidentiality of non-discoverable matters, and costs. FED. R. CIV. P. 34 advisory committee's note.

in its production.[6] In 2002, the United States Judicial Conference Advisory Committee on Civil Rules asked for comments concerning whether an amendment to the Federal Rules of Civil Procedure was needed due to the introduction of electronic data such as e-mail and word processing files into the business world.[7] Even with new rules governing discovery of electronically-stored information, the application of the various discovery rules becomes complicated when electronic data is sought because much of the information may be available only on backup tape or disc storage systems. In these situations, those called upon to produce usually argue that the possibility that a search of the company's backup tapes will yield relevant evidence is so remote that it cannot possibly justify the costs involved.[8]

[9] Fortunately, just as with traditional paper-based discovery, the limitations with respect to reasonableness, convenience, burden, and expense all apply to electronic information. The Federal Rules of Civil Procedure provide that courts may limit the frequency or extent of use of the discovery methods otherwise permitted under the rules and by any local rule if it determines that:

> (i) the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive; (ii) the party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought; or (iii) the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs

---

[6] *See, e.g.*, CAL. CIV. PROC. CODE § 2031(g)(1) (2003) (shifting the expense of translating data compilations into reasonably usable form to the demanding party); TEX. R. CIV. P. 196.4 (2003) (providing that one must specifically request data in electronic form, that respondents be required to produce only what is "reasonably available" in the "ordinary course of business," and allowing objections for unreasonable requests, and cost shifting for reasonable expenses of any extraordinary steps); ILL. SUP. CT. R. 201(b)(2) (2004) (permitting apportionment of costs of retrieval of information including attorneys' fees).

[7] Thomas Y. Allman, *Electronic Evidence, Discovery: A Primer*, *in* 6 NAT'L LEGAL CENTER FOR THE PUBLIC INT., BRIEFLY… PERSPECTIVES ON LEGISLATION, REGULATION, AND LITIGATION 11, Nov. 2002 (calling for cost-shifting to the requesting party requiring it to pay the reasonable expenses of any extraordinary steps required to retrieve and produce the information).

[8] *See, e.g.*, McPeek v. Ashcroft, 202 F.R.D. 31, 32 (D.D.C. 2001) (applying the above-mentioned rule).

> 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.[9]

Accordingly, any party who believes the burdens or expense of the discovery outweighs the benefit of the discovery should invoke Federal Rule of Civil Procedure 26(b)(2)(iii).[10]

[10] The traditional limitations on document discovery comprise the foundation upon which the limitations on electronic discovery have been built and therefore are essential to understanding the challenges that exist in responding to a request for the production of electronic information. Under the Federal Rules of Civil Procedure as they relate to discovery, courts must start with the presumption that the responding party must bear the expense of complying with discovery requests.[11] This principle, while unassailable in the context of paper records, is not as effective when it comes to electronic data.[12] A company may store paper documents because the information is useful to it, and that use validates the cost of retention. Accordingly, it is not inappropriate to expect the party to locate the information, whether for its own needs or in response to a discovery request.[13] However, a company may store electronic data, not always for purposes of its use, but because the cost of storing it is relatively inexpensive; data is often stored not because the company expects to use it but because there "is no compelling reason to discard it."[14]

[11] Courts have devised "creative" ways to balance the broad scope of discovery permitted by Rule 26(b)(1) with the cost-consciousness of Rule 26(b)(2).[15] For example, there is no controlling authority for the proposition that restoring all back up tapes is necessary in every case.[16] Some courts have said that producing backup tapes is a cost of doing

---

[9] FED. R. CIV. P. 26(b)(2).

[10] The Rule allows the court to limit discovery based upon undue burden or expense.

[11] Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340, 358 (1978).

[12] Rowe Entm't, Inc. v. William Morris Agency, Inc. 205 F.R.D. 421, 429 (S.D.N.Y. 2002).

[13] *Id*.

[14] *Id*.

[15] Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 316 (S.D.N.Y. May 13, 2003).

[16] McPeek v. Ashcroft, 202 F.R.D. 31, 33 (D.D.C. 2001).

business in the computer age.[17] Other courts have shifted the cost, forcing the requesting party, rather than the answering party, to bear the cost of discovery, in certain situations.[18]

[12] Essentially, courts have taken different approaches in determining whether to shift the cost of production. Those standards include the proportionality test set forth in Federal Rule of Civil Procedure 34. That Rule allows a party to object to a request for production, and thereby protects a party producing electronic evidence against undue burden and expense associated with the production. In addition, courts have utilized some new standards and approaches to address concerns of undue burden and expense as questions and issues surrounding e-discovery have increased.

B. *There are Four Approaches Used by Courts.*

1. The Cost Based Approach

[13] The Cost Based Approach is also termed the "market" economic approach. The Cost Based Approach supposes that charging the requesting party would guarantee that the requesting party would only demand what it needs.[19] As one court noted, "American lawyers engaged in discovery have never been accused of asking for too little. To the contrary, like the Rolling Stones, they hope that if they ask for what they want, they will get what they need."[20] Those who favor a "market" economic approach argue that charging the requesting party guarantees that the requesting party would only demand what it needs. The party seeking the restoration of the backup tapes pays for them. Thus, the requesting party literally gets what it pays for.[21]

2. The Marginal Utility Approach

[17] *Id*. at 33 (citing *In re* Brand Name Prescription Drugs, No. 94 C 897, 1995 WL 360526 at *3 (N.D. Ill. June 15, 1995)).

[18] Murphy Oil USA, Inc. v. Fluor Daniel, Inc., No. 99-3564, 2002 U.S. Dist. LEXIS 3196, at *9 (E.D. La. Feb. 29, 2002).

[19] *McPeek,* 202 F.R.D. at 34.

[20] *Id*. at 33-34.

[21] *Id.* at 34 (citing Marnie H. Pulver, Note, *Electronic Media Discovery: The Economic Benefit of Pay-Per-View*, 21 CARDOZO L. REV. 1379 (2000)).

[14] Another method is the so-called "marginal utility" approach, which some courts have adopted as a more fair approach to cost-shifting.[22] Using this economic principle, courts attempt to strike a balance. The more likely it is that backup tapes contain information relevant to a claim or defense, the more fair it is that the producing party search at its own expense. The less likely it is, the less fair it would be to charge the producing party for the search. The difference is "at the margin."[23]

[15] Using the marginal utility approach, courts may order a test run, ordering the producing party to perform a backup restoration of the e-mails attributable to a principal witness in the lawsuit for a limited period of time. The company is then ordered to document the time and money spent performing the search and to search the restored e-mails for documents responsive to the discovery request for production of documents. Once completed, the company files a comprehensive, sworn statement of the expenses incurred and the results achieved. The court often permits the parties to argue why the results and the expenses do or do not justify a further search.

3. The *Rowe* Test

[16] In January of 2002, the United States District Court for the Southern District of New York set forth an eight factor test to ascertain whether and to what extent costs associated with complying with onerous discovery requests should be shifted to the requesting party.[24] *Rowe* involved African American concert promoters who contended that they were denied the opportunity to promote white music artists by the allegedly discriminatory and anti-competitive practices of talent agencies and concert promoters.[25] All of the defendants responded to the plaintiffs' requests and each permitted inspection of files related to the concert promotions.[26] Four sets of defendants moved pursuant to Federal Rules 26(b)(2)(iii) and 26(c) for a protective order relieving them of the obligation to produce e-mail that may have been responsive to the

[22] *Id.*
[23] *Id*.
[24] Rowe Entm't, Inc. v. William Morris Agency, Inc., 205 F.R.D. 421, 429 (S.D.N.Y. 2002).
[25] *Id.* at 423.
[26] *Id.*

discovery requests.[27] The four sets of defendants each estimated the cost of production as anywhere from 250 to 400 thousand dollars and asked that the plaintiffs bear the cost.[28] The Court used a balancing test derived from prior case law to determine whether to shift the cost of production.[29]

[17] The eight factors in the test are as follows:

1) The specificity of the discovery requests – the less specific, the more appropriate the court found it to shift the cost to the requestor;

2) The likelihood of discovering critical information – using the marginal utility test set forth in *McPeek v. Ashcroft*;

3) The availability of such information from other sources – if kept only for purposes of an emergency then cost shifting is warranted;

4) The purposes for which the responding party maintains the requested data;

5) The relative benefits to the parties of obtaining the information – if respondent benefits then the costs should not be shifted;

6) The total cost associated with production – if not substantial there is no need to shift the cost;

7) The relative ability of each party to control costs and its incentive to do so – if discovery is incremental then cost should be placed on the requesting party; and

8) The resources available to each party – if production will economically damage one party more then the court should shift the cost to the other.[30]

---

[27] *Id.* Co-Author Stephen Williger represented some of the independent concert promoters who objected to the production.

[28] *Id.* at 425.

[29] *Id.* at 429.

[30] *Id.*

[18] The *Rowe* court decided that the factors tipped heavily in favor of shifting the costs of production to the plaintiffs, and the Court required them to pay for the recovery and production of defendants' extensive e-mail backups. The defendants, as respondents, had to bear the cost of the relevance and privilege review.[31]

[19] A federal court in Louisiana, following the *Rowe* decision, also shifted the cost to the party seeking the discovery.[32] In *Murphy Oil USA, Inc. v. Fluor Daniel, Inc*., a breach of contract action, the plaintiff sought to compel production of certain e-mails it claimed were responsive to discovery requests.[33] The plaintiff's request covered e-mails of thirty-seven company employees who had worked on a project at issue in the lawsuit.[34] The e-mails were available only on backup tapes.[35] The respondent-company contended that the expense of production outweighed the benefit of the evidence and asked that the court shift the costs of production to the plaintiff.[36] The backup tapes contained e-mails from the thirty-seven employees involved in the disputed work, as well as from the defendant's 650 other employees.[37] Each tape contained an estimated 25,000 e-mails.[38] The defendant produced an estimate that it would take six months and $6.2 million to restore the tapes, convert the e-mails to TIFF images, and print the e-mails.[39]

[20] The court, relying upon the *Rowe* factors, concluded that only two of the factors favored allocating costs to the producing party: the specificity of the plaintiff's request and the unavailability of the e-mails from other sources.[40] The other five factors favored shifting the cost to the party seeking discovery.[41] Those factors included: the "modest" likelihood of

---

[31] *Id*. at 433.

[32] Murphy Oil USA, Inc. v. Fluor Daniel, Inc., No. Civ. A. 99-3564, 2002 WL 246439, at *7-*8 (E.D. La. Feb. 19, 2002).

[33] *Id.* at *1.

[34] *Id.*

[35] *Id.* at *2.

[36] *Id.* at *1.

[37] *Id.* at *1-*2.

[38] *Id*. at *2.

[39] *Id*. at *4.

[40] *Id.* at *5.

[41] *Id.* at *6.

retrieving relevant information, the lack of a business purpose for retention of the tapes or benefit to the defendant in restoring them, the magnitude of the total cost, and the plaintiff's ability to control costs by paring its request.[42] The court ordered the requesting party to pay the costs of restoring and printing the e-mails.[43] In response to its concern that the plaintiff would gain access to privileged or confidential information, the court gave the responding party two choices.[44] The first allowed the defendant-respondent to forego a prior review of e-mail recovered at the plaintiff's expense; the second allowed the defendant to review, at its own cost, all relevant documents recovered by the expert before production to the plaintiff.[45]

4. The *Zubulake* Factors.

[21] In May of 2003, the court in the Southern District of New York recognized that *Rowe* had become the "gold standard" of review, but was concerned that the *Rowe* standard was undercutting the presumption that the responding party pays the cost of production.[46] In response, the court modified the *Rowe* test to combine some of the factors, and created a new seven factor test to consider when deciding whether to shift the cost of production.[47] In making the modification, the court in *Zubulake v. UBS Warburg, LLC* recognized that "cost-shifting may effectively end discovery, especially when private parties are engaged in litigation with large corporations."[48] The court worried that, as large companies move increasingly toward paper-free environments, the frequent use of cost-shifting will have the effect of crippling discovery in discrimination and retaliation cases.[49] The court further stated that this will undermine the "strong public policy favor[ing] resolving disputes on their merits," and may ultimately deter the filing of potentially meritorious claims.[50]

---

[42] *Id.* at *6-*7.
[43] *Id.* at *8-*9.
[44] *Id*. at *8.
[45] *Id*. at *8-*9.
[46] Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 320-21 (S.D.N.Y. 2003).
[47] *Id* at 322.
[48] *Id*. at 317.
[49] *Id.* at 317-18.
[50] *Id*. at 318.

[22] *Zubulake* involved an equities trader who earned approximately $500,000 a year.[51] She sued for gender discrimination, failure to promote, and retaliation under federal, state, and city law.[52] To support her claims, Zubulake sought information on UBS's backup tapes – mostly e-mails sent about her.[53] The question again before the court was who should pay the cost incurred in restoring and producing backup tapes – Zubulake, as the party seeking the discovery, or the company, as respondent.[54]

[23] In May of 2003, the court ordered the defendants to restore and produce e-mail from five of the ninety-four backup tapes at defendant's cost.[55] UBS came back in July and asked that the costs of further production, estimated at $273,000, be shifted to Zubulake.[56] In weighing the merits of shifting the cost of production, the *Zubulake* court stated that cost shifting is only appropriate for "inaccessible" material. For example, it would not be appropriate to shift the cost of producing active on-line data or near line data.[57] The court also held, as others consistently do, that the responding party has the burden of proof on cost shifting.[58]

[24] In determining whether to shift the cost of production, the *Zubulake* court considered the following seven-factor test:

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;

[51] *Id.* at n.9.
[52] *Id*. at 311-12.
[53] *Id.* at 312.
[54] *Id.* at 317-18.
[55] *Id.* at 323-24.
[56] *Id.*
[57] *Id*. at 323.
[58] *Id*. at 324.

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.[59]

[25] The first two factors of the *Zubulake* test comprise the "marginal utility test" utilized in *McPeek v. Ashcroft* and discussed above, and the *Zubulake* court found that this test should be weighted most heavily in the cost-shifting analysis.[60] Factors three, four, and five address cost issues – the expense of the production and who can best handle the expense. The court stated that, where cost shifting is appropriate, only the costs of restoration and searching should be shifted.[61] The responding party always bears the cost of reviewing and producing electronic data once it has been obtained and converted.[62] The court eventually ordered that UBS pay 75% of the cost of production and Zubulake 25%.[63] However, the court also suggested that UBS could potentially impose a shift of all of its costs, including attorneys' fees, by making an offer of judgment to Plaintiff pursuant to Rule 68 of the Federal Rules of Civil Procedure.[64]

III. IDENTIFICATION, PRESERVATION, AND COLLECTION OF ELECTRONIC INFORMATION

A. *Identification*.

[26] Responding to discovery in a paper world usually means looking through a number of files organized by chronology, subject, or person. While time consuming, it was and is a relatively simply task. Meanwhile,

---

[59] *Id.*
[60] *Id*. at 323.
[61] *Id.*
[62] Zubulake v. UBS Warburg LLC ("Zubulake II"), 216 F.R.D. 280, 284 (2003).
[63] *Id.* at 284-85.
[64] *Id*. at 291; *see* FED. R. CIV. P. 68 ("At any time more than 10 days before the trial begins, a party defending against a claim may serve upon the adverse party an offer to allow judgment to be taken against the defending party for the money or property or to the effect specified in the offer with costs then accrued. . . . If the judgment finally obtained by the offeree is not more favorable than the offer, the offeree must pay the costs incurred after the making of the offer.").

backup tapes of electronic documents collect data indiscriminately, regardless of topic, author, or subject. They span a company's system and are oftentimes disposed of or taped over after a relatively short period of time. That makes collecting documents responsive to discovery requests expensive, not only monetarily, but also in terms of the effort required to accomplish the task.

[27] The first step in responding to electronic discovery requests is the same as with traditional discovery: requests for information should be sent to all responsible persons so that appropriate measures can be implemented to identify, preserve, and collect all potentially relevant information. While that may seem to be easy, it is not. Each of these steps will likely require the involvement of those responsible for a company's information technology systems, because technology-centric collection of information may require case- and issue-specific suspension of automated electronic document destruction facilities.

[28] The nature of this problem is perhaps best illustrated by looking at the different types of electronic information that could be subject to production.[65] However, even this inquiry is not as simple as it may first appear. In fact, courts that have dealt with these very issues have struggled to come up with a uniform classification of the different types of electronic information that are subject to production. In some instances, courts will look to the *type* of electronic information in determining how the discovery rules should apply.[66] Among the different types considered are the following:

---

[65] *See, e.g.*, McPeek v. Ashcroft, 202 F.R.D. 31, 34 (D.D.C. 2001). The court noted that parties should seek judicial intervention if they believe an electronic discovery request is being used merely as a litigation tactic. *Id.* The responding party may invoke the court's discretion under Rule 26(c) to grant orders protecting it from "undue burden or expense" in complying with the request, including orders conditioning discovery on the requesting party's payment of the costs of discovery. *Id.* Companies that refuse on their own to search backup tapes for additional electronic evidence face the possibility that the trial judge may give a jury instruction that this failure to search permits the inference that the unfound files would contain information detrimental to the non-producing party. *Id.*; *see also* Trigon Ins. Co. v. United States, 204 F.R.D. 277, 289 (E.D. Va. 2001) (finding it appropriate that the United States was held responsible for its litigation support firm's intentional spoliation and adverse inferences regarding the content of the destroyed electronic documents).

[66] One constant is that routine recycling of computer storage media must halt during discovery when that is the most reasonable means of preserving data. Failure to preserve e-mail and electronic documents can be sanctioned as spoliation of evidence even if it is

- *Electronic Documents*. This category encompasses those documents intentionally created by a computer user, including word processing documents, spreadsheets, presentations, and the like.
- *E-Mail*. The proliferation of e-mail as a means of communication has greatly increased the amount of information that may be discoverable. Without e-mail, interaction is conducted face-to-face and by telephone and no discoverable record is created. With e-mail, communication is conducted electronically and copies of the communication are retained on both the sender's and the recipient's computers.
- *"Hidden" Information*. "Hidden" information includes generally electronic information created or maintained on a computer that was not intentionally created by the computer user but instead was created or maintained automatically by the computer. Hidden information includes: Meta-data, system logs, temporary files, and "cookies."
- *Backup Files*. As a matter of good information management practice, many companies routinely create backup copies of their computer systems for disaster recovery purposes.

[29] Other courts, instead of looking to the type of electronic information or its intended use, will examine the means by which the information is used and maintained in the ordinary course of business. For example, the court in *Zubulake* identified five categories of electronic information and classified each as to the means by which such information could be accessed.[67] Those categories include:

- *Active, online data*: "On-line storage is generally provided by magnetic disk. It is used in the very active stages of an electronic records [sic] life – when it is being created or received and processed, [or] when the access frequency is high and the required speed of access is very fast, i.e., in milliseconds."[68] Examples of online data include hard drives.

---

inadvertent. Metro. Opera Assoc., Inc. v. Local 100, 212 F.R.D. 178, 181-82, 231 (S.D.N.Y. 2003).

[67] Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 318-19 (S.D.N.Y. 2003).

[68] COHASSET ASSOCS., TRUSTWORTHY STORAGE AND MANAGEMENT OF ELECTRONIC RECORDS: THE ROLE OF OPTICAL STORAGE TECHNOLOGY (Apr. 2003), *at*

- *Near-line data*: "This typically consists of a robotic storage device (robotic library) that houses removable media, uses robotic arms to access the media, and uses multiple write/read devices to store and retrieve records."[69] Access speeds vary from milliseconds for media already in a read device, to thirty seconds for optical disk technology, to as long as two minutes for sequentially searched media, such as magnetic tape.
- *Offline storage/archives*: As defined by Cohasset Associates, one of the nation's leading information management consulting firms, offline or archival data is:

> [R]emovable optical disk or magnetic tape media, which can be labeled and stored in a shelf or rack. Off-line storage of electronic records is traditionally used for making disaster copies of records and also for records considered 'archival' in that their likelihood of retrieval is minimal. Accessibility to off-line media involves manual intervention and is much slower than on-line or near-line storage. Access speeds may be minutes, hours, or even days, depending on the access-effectiveness of the storage facility.[70]

The principle difference between nearline data and offline data is that offline data lacks "the coordinated control of an intelligent disk subsystem," and is, in the nomenclature of technology experts, JBOD ("Just a Bunch of Disks").[71]

- *Backup tape*: As defined by the *Zubulake* court, a backup tape is:

> A device, like a tape recorder, that reads data from and writes it

---

http://www.hp.com/products1/storage/products/archivalprod/whitepapers/trustworthy_storage.pdf.) (last visited Feb. 6, 2004).

[69] *Id.*

[70] *Id.*

[71] CNT, THE FUTURE OF TAPE, *at* www.cnt.com/literature/documents/pl556.pdf (last visited Feb. 6, 2004).

> onto a tape. Tape drives have data capacities of anywhere from a few hundred kilobytes to several gigabytes. Their transfer speeds also vary considerably. . . The disadvantage of tape drives is that they are *sequential-access* devices, which means that to read any particular block of data, you need to read all the preceding blocks.[72]

As a result, "[t]he data on a backup tape are not organized for retrieval of individual documents or files [because] . . . the organization of the data mirrors the computer's structure, not the human records management structure."[73] Backup tapes also typically employ some type of data compression, permitting more data to be stored on each tape, but also making restoration more time-consuming and expensive, especially given the lack of uniform standard governing data compression.[74] All data on each backup tape must be restored from the backup tape format to a format that the standard computer can read. In the case of a large data volume on multiple tapes the restored files from each tape must be compared to the restored files from every other tape and duplicate files eliminated. The restored data files that are not duplicates must be converted to a common format so that a search program may seek information within them.[75] Once the backup tapes have been restored to a disk or hard drive from which they can be read, someone has to review the restored file, whether a word-processing document or e-mail, and

---

[72] *Zubulake*, 217 F.R.D. at 319-20 n.55 (quoting Webopedia, *at* http://inews.webopedia.com/TERM/t/tape_drive.html (last modified June 21, 2002)).

[73] *Id*. at n.56 (quoting Kenneth J. Withers, Computer-Based Discovery in Federal Litigation 15 (unpublished manuscript)).

[74] *Id*. at n.57 (citing SDLT, *Making a Business Case for Tape*, *at* http://quantum.treehousei.com/Surveys/publishing/survey_148/pdfs/making_a_business_case_for_tape.pdf (June 2002); Jerry Stern, *The Perils of Backing Up, at* http://www.grsoftware.net/backup/articles/jerry_perils.html (last modified Feb. 27, 2002)).

[75] *Id*.

determine whether it falls within one of the discovery requests.[76]

- *Erased, fragmented or damaged data*: Namely,

> When a file is first created and saved, it is laid down on the [storage media] in contiguous clusters. . . . As files are erased, their clusters are made available again as free space. Eventually, some newly created files become larger than the remaining contiguous free space. These files are then broken up and randomly spaced through the disk.[77]

Such broken-up files are said to be "fragmented," and, along with damaged and erased data, can only be accessed after significant processing.[78]

[30] Some courts have recognized that backup tapes are not created for record retrieval purposes, but rather to allow for system reconstruction in the case of disasters.[79] In such situations, it is less likely that a court will force a respondent to pay for the cost of producing the data. It is when a party maintains electronic data for the purpose of utilizing it in connection

---

[76] McPeek v. Ashcroft, 202 F.R.D. 31, 32 (D.D.C. 2001).

[77] *Zubulake*, 217 F.R.D. at 319-20, n.58 (quoting Sunbelt Software, *White Paper: Disk Defragmentation for Windows NT/2000: Hidden Gold for the Enterprise* 2, *at* http://www.sunbelt-software.com/evaluation/455/web/documents/idc-white-paper-english.pdf (Last visited Jan. 23, 2004)).

[78] *Id*. at 319-20 n.59 (citing Executive Software International, *Identifying Common Reliability/Stability Problems Caused by File Fragmentation*, *at* http://www1.execsoft.com/pdf/stability_WhitePaper.pdf (last visited Jan. 23, 2004) (identifying problems associated with file fragmentation, including file corruption, data loss, crashes, and hard drive failures); Stan Miastkowski, *When Good Data Goes Bad*, PC World, *available at* http://www.pcworld.com/resource/printable/articles/O,aid,13859,00.asp (Jan. 2002).

[79] Rowe Entm't, Inc. v. William Morris Agency, Inc. 205 F.R.D. 421, 431 (S.D.N.Y. 2002) ("[A] party that happens to retain vestigial data . . . only in case of an emergency or simply because it has neglected to discard it, should not be put to the expense of producing it."). The court reiterated that requiring a producing party in discovery to seek deleted e-mails from a hard drive is no more necessary than requiring a party "to sort through its trash to resurrect discarded paper documents." *Id*. This assumes, of course, that hard copy and electronic documents are not discarded to avoid their discovery.

with its current activities that the party may be expected to respond to discovery requests at its own expense.[80]

[31] Courts also recognize, with regard to the issue of searching backup tapes, that "[t]he likelihood of finding relevant data has to be a function of the application of the common sense principle that people generate data referring to an event, whether e-mail or word processing documents, contemporaneous with that event . . . ."[81] Accordingly, those subject to a document request asking for backup files must be ready to argue that the request be limited to certain back up tapes which span the relevant time period. Preparation may be the difference between convincing a judge that searching only some versus all of the company's backup tape is appropriate. It could mean the difference between spending thousands of dollars versus millions of dollars in responding to discovery.

B. *Review of Collected Information*.

[32] The quantity of information collected in response to a discovery request covering electronic materials is typically massive. Moreover, the methods used to collect the information can impact significantly the costs associated with review for relevance, privilege, and confidentiality. In particular, it is much more efficient to collect and review native-file copies of documents as opposed to hard-copy printouts. Native-file copies can be full-text searched, which can reduce the costs associated with review and the use of the materials throughout the litigation. Further, as already stated, native-file copies of documents may contain information that does not appear on hard-copy printouts, such as document metadata and e-mail header information.

[33] While courts have shifted the cost of producing electronic documents to the party demanding the production, the issue of who should pay the cost to identify privileged and confidential communications contained within the backup systems is often allocated to the producing party. The district court in *Rowe* held that any defendant who elects to conduct a full privilege review of its e-mails prior to production, must do so at its own

[80] *Id*. at 430.

[81] *McPeek*, 212 F.R.D. at 35 (stating that it is unlikely that people, working in an office, generate data about an event that is not contemporaneous, unless they have been charged with the responsibility to investigate that event or to create some form of history about it).

expense.[82] Accordingly, based upon the holding in *Rowe*, the full cost of retrieval from the backup tapes would be borne by the party who wanted to conduct a privilege review prior to production.

[34] Other courts, however, have parted company with that position and have held that the producing party must have an opportunity to assert that the e-mail is confidential or privileged without bearing the cost of retrieving the e-mail.[83] However, those courts provide that the producing party would have to bear the cost of separating pertinent e-mails from the non-responsive e-mails and identifying the privileged or confidential e-mails found within the pertinent e-mails.[84]

C. *Form of Production of Responsive Materials*.

[35] Traditionally, documents only were produced in hard copy format. The nature of digitally maintained information expands available options, with a corresponding expansion of the considerations relating to production. The Federal Rules of Civil Procedure require production of documents as they are maintained in the ordinary course of business.[85] Does this rule require the production of exact digital copies, or will hard copies or limited digital copies suffice?

[36] Case law is split on whether a party is entitled to discovery of electronic versions as well as hard copy paper versions of computer files.[86] Rule 34 of the Federal Rules of Civil Procedure may require production of computer data in machine-readable form in addition to providing hard copy printouts of that information.[87] Exact digital copies can be

---

[82] *Rowe*, 205 F.R.D. at 432.

[83] *See*, *e.g.*, Murphy Oil USA, Inc. v. Fluor Daniel, Inc., No. Civ. A. 99-3564, 2002 WL 246439, at *8 (E.D. La. Feb. 19, 2002).

[84] *See id.*

[85] FED. R. CIV. P. 34(b).

[86] Medtronic Sofamor Danek, Inc. v. Michelson, No. 01-2373-M1V, 2003 WL 21468573, at *5-*6 (W.D. Tenn. May 13, 2003).

[87] *See, e.g.*, Adams v. Dan River Mills, Inc., 54 F.R.D. 220, 222 (D. W.Va. 1972) ("Because of the accuracy and inexpensiveness of producing the requested documents in the case at bar, this court sees no reason why the defendant should not be required to produce the computer cards or shapes and the W-2 printouts to the plaintiffs."); *see also* Simon Property Group L.P. v. mySimon, Inc., 194 F.R.D. 639, 640 (D. Ind. 2000) ("First, computer records, including records that have been 'deleted,' are documents discoverable under Fed. R. Civ. P. 34."); Bills v. Kennecott Corp., 108 F.R.D. 459, 461 (D. Utah 1985) ("It is now axiomatic that electronically stored information is discoverable under

manipulated in ways that are difficult to detect. If proprietary file formats are used, the producing party may be required to make available the tools necessary to view the files.

[37] Electronic records may contain data that the hard copy does not include. Important information present in the computer system regarding who sent the document, when he or she sent it, and to whom the document was sent will not always be preserved in the paper printout. The Advisory Committee Notes to Federal Rule of Civil Procedure 34 make it clear that information stored in computer format is discoverable.[88] Because the electronic data files could reasonably lead to the discovery of admissible evidence that is not available from a hard copy, courts will find this to be a factor weighing in favor of a respondent paying for the cost of production.[89]

[38] The United States District Court for the Southern District of California has noted that the only restriction on the discovery is that the producing party may be protected against undue burden and expense and/or the invasion of privileged matter.[90] To protect privilege, confidentiality, and the integrity of the evidence, courts will sometimes appoint a qualified neutral computer expert to conduct discovery of the defendant's computer hard drive. Often, the time, cost, and intrusiveness associated with the production are far greater than originally estimated.[91]

IV. WHAT'S A COMPANY TO DO?

A. *Overview of Most Pressing Concerns That Can Be Addressed.*

[39] One of the most pressing concerns that companies responding to electronic discovery requests face is downtime in operations. A short four- to five-hour shutdown in order to recover information from a

Rule 34 of the Federal Rules of Civil Procedure if it otherwise meets the relevancy standard prescribed by the rules . . . .").

[88] FED. R. CIV. P. 34 advisory committee's note.

[89] *See Medtronic*, 2003 WL 21468573, at *5-*6.

[90] *See, e.g.*, Playboy Enters., Inc. v. Welles, 60 F. Supp. 2d 1050, 1053 (S.D. Cal. 1999).

[91] *See* Northwest Airlines v. Local 2000, International Brotherhood of Teamsters, No. Civ. 00-08, 2000 WL 33419439, at *2 (D. Minn. 2000) (noting the court's establishment of a cut-off date for discoverable materials, but nevertheless permitting a very broad swath of discovery).

company's hard drive can mean significant lost profits and additional costs in employee expenditures.

[40] Rule 34 of the Federal Rules of Civil Procedure requires, at a minimum, locating all sources and locations of electronic data.[92] Data will commonly be located on individual desktops and laptops, network hard discs, removable media such as floppy discs, tapes, and CDs, and, increasingly, personal digital assistants such as hand held computers. Data may also be in the possession of third parties, such as Internet service providers, and on the computer systems of other entities outside the corporation.[93]

[41] Determining the volume of e-mail and other electronic information is crucial, but it can be difficult to do without the assistance of an experienced electronic discovery expert. In order to comply with a typical electronic discovery request, a respondent will have to engage in a three-step process: cataloging, restoring, and processing.[94] Cataloging involves identifying the tapes that contain the e-mail files and marking them for restoration.[95] Restoration consists of saving all relevant documents from the identified files to a master database and then removing the duplicates.[96] Processing involves making the files readable on a computer screen but also printable so that they can be Bates-labeled for production.[97]

B. *Have a Plan in Place Before the Need Arises*.

[42] Federal Rule of Civil Procedure 26(f) provides that parties who have suits pending in federal court must meet early in the process to discuss

---

[92] FED. R. CIV. P. 34.

[93] *See generally* Electronic Evidence Discovery & Computer Forensics Software and Services by Kroll, Kroll On Track, *at* http://www.krollontrack.com (last visited Feb. 6, 2004) (detailing the services of one such entity, which can provide specialized services dealing with electronic discovery).

[94] Murphy Oil USA, Inc. v. Fluor Daniel, Inc., No. Civ. A. 99-3564, 2002 WL 246439, at *4 (E.D. La. Feb. 19, 2002).

[95] *Id.*

[96] *Id.*

[97] *Id*.

various issues of import to the litigation.[98] One of the tasks the parties are charged with is to develop a proposed discovery plan:

> In the electronic age, this 'meet and confer' should include a discussion on whether each side possesses information in electronic form, whether they intend to produce such material, whether each other's software is compatible, whether there exists any privilege issue requiring redaction, and how to allocate costs involved with each of the foregoing.[99]

[43] That guideline can assist companies in helping to formulate their plans for preserving electronic discovery. A party who has been sued or who has filed suit may be required to submit a proposed discovery protocol to the court as early as possible. In addition, it may be necessary that those submitting such a protocol provide statements from technology professionals at the company in support of the proposal. The court will then likely review the proposal along with the opponents and craft a discovery plan by which both parties must abide.

[44] Courts that have addressed the issue have recognized various types of discovery protocols in electronic discovery cases. In cases where the producing party elects not to review the communications on the backup tapes prior to production, the following protocol has been described:

- The producing party produces a log of the backup tapes that identifies the dates of the e-mail communications at issue and the party which has propounded the discovery selects one of the backup tapes.

- The party seeking the discovery then designates one or more experts to retrieve the e-mail from the selected backup tape, subject to objection by the producing party. Once an expert has been agreed to, the backup tape is delivered.

- Counsel for the party seeking production shall then review the e-mail communications retrieved, identify which e-mail is

[98] FED. R. CIV. P. 26(f).

[99] *In re* Bristol-Myers Squibb Securities Litigation, 205 F.R.D. 437, 444 (D.N.J. 2002).

responsive to their discovery, and provide it to the producing party with bates numbers and the back up tape. (The party seeking production shall bear the expense.)

- The producing party shall then review the documents and designate in a privilege log any documents that are proprietary, any that contain attorney-client communications, any that represent the work product of an attorney, and those documents that are discoverable. Any documents determined by both counsel to be proprietary are subject to a protective order, and those deemed privileged and still in the hands of the opposing counsel shall be destroyed.

- The parties must seek the court's intervention in case of disagreements as to what documents are responsive and what are non-discoverable.[100]

[45] Courts have recognized a second protocol if the producing party elects to review the e-mail communications on the backup tapes prior to production. The first two steps are the same as set forth above except that the compelling party's expert must agree in writing that he or she shall not disclose to the party or its counsel any information pertaining to the substance of the e-mail communications until after the proprietary and privilege issues are resolved.

- The expert selected, at the expense and direction of the party seeking production, shall retrieve the e-mail communications on the selected back up tape.

- At its expense, the producing party shall review the e-mail communications retrieved and cull out those e-mail documents that are not responsive to the discovery requests and which are privileged or proprietary.

- After a review of the log setting forth claimed privilege and/or proprietary information, if there is agreement then it shall be subject to the terms of the protective order set forth above.

[100] *See Murphy Oil*, 2002 WL 246439, at *8-*10 (applying the protocol to respondents).

- If there is disagreement then the parties are to seek judicial intervention.[101]

[46] In some cases, courts have taken it upon themselves to craft the protocol. In *Playboy Enters., Inc. v. Welles,* the court, noting that the defendant's own actions in deleting incoming and outgoing e-mails were partly to blame for the dispute, ordered that an expert, paid for by the party seeking production, be employed to determine whether some of the deleted e-mail could be recovered.[102] The parties were required to agree upon and employ a computer expert who specializes in the field of electronic discovery to create a "mirror image" of the defendant's hard drive.[103] After the hard drive was mirrored, the expert was to give it to defendant's counsel who would print and review any recovered documents.[104] The defendant's attorney had to produce to the plaintiff's counsel any responsive communications.[105] Any documents that were withheld based upon privileged or propriety information were to be noted in a privilege log.[106]

[47] With all the confusion about what electronic data is subject to production, companies must be cognizant of the fact that they may be questioned about the electronic documents they produce. Many attorneys will serve interrogatories on, or take the deposition of, the producing party, questioning whether it has overwritten or revised any relevant documents since the beginning of the dispute. Responses can be a powerful weapon that can carry significant consequences. Another tool parties are utilizing more frequently is the motion to compel, specifically as a means by which to enforce the production of electronic data. Parties are also resorting to hiring computer experts to determine whether the data is being produced in an altered state. If alterations are proven, then spoliation claims often follow. Parties likewise are seeking protective orders from the courts in order to prevent the destruction of electronic data. One court recently granted an *ex parte* application for a preliminary injunction which effectively put a "freeze" on defendants' electronically

[101] *Id*.

[102] Playboy Enters., Inc. v. Welles, 60 F. Supp. 2d 1050, 1053 (S.D. Cal. 1999); See also *mySimon, Inc*., 194 F.R.D. at 64 (adopting the protocol utilized by the court in *Welles.*).

[103] *Welles*, 60 F. Supp. 2d at 1055.

[104] *Id.*

[105] *Id.*

[106] *Id.*

stored data so that it would be available for future discovery, thereby avoiding possible destruction of that evidence during what might be innocent, routine document disposal practices of defendants.[107]

[48] Electronic evidence creates new and unique ways for companies to unwittingly destroy evidence. There are many means by which respondents can get themselves in trouble with the court when copying data for production or review. Failure to make sector-by-sector images prior to viewing may result in a spoliation claim. Simply "booting" a computer can destroy "slack" and "temporary" files.

[49] Clicking on a file rather than properly copying it can change its last access date and lead to harsh sanctions or inadmissibility.[108] These are reasons why it is important to have a sound document retention and production plan in place. Companies should consider having a knowledgeable computer systems analyst, administrator, or engineer on staff or retained who understands the company's systems and how to produce the data in pure form.

[50] The average person in a company is not computer literate enough to know how to protect the company from inadvertent spoliation. Accordingly, it is important that companies be prepared to retain a discovery expert, used in the records-custodian capacity, who can perform the tasks necessary to insure that electronic data is being properly maintained. Companies also need to be informed when hiring a law firm to represent them should they be sued or believe they will be sued. A law firm that is properly educated in the area of electronic data production is important in this electronic age. Some law firms recommend that the firm itself be the entity to hire the electronic discovery expert so that counsel can then argue that all of the experts' duties fall squarely within the work-product doctrine.[109]

---

[107] Dodge, Warren & Peters Ins. Servs. v. Riley, 130 Cal. Rptr. 385, 388 (Cal. Ct. App. 2003).

[108] *Kroll*, *supra* note 93.

[109] Many firms also recommend hiring an additional expert for cases that require expert computer-forensic work. The purpose of that expert is only to formulate and present opinions as to the evidence. It may be wise for companies to keep any other opinion experts separate from computer experts who perform hands-on collection or processing of electronic information.

C. *Address and Control Your Company's Culture Concerning Electronic Documents*.

[51] The most important step for a company to take is to update or institute a corporate retention policy for electronic records. Such a policy is necessary to enable a company to meet the current challenges of discovery. A company's in-house counsel may be viewed as having an obligation to affirmatively advise his or her client that the company should have a reasonable system of e-document retention to maintain any materials that may legitimately be the subject of discovery in possible future claims. If a company is sued, there is an obligation to tell the client to save e-documents that may be relevant to the claims.[110]

[52] Courts have imposed liability on defendants and have ordered defendants to pay plaintiffs' attorney fees if defendants fail to preserve and produce electronic documents.[111] Courts will consider ordering the responding parties to pay attorney fees and the costs expended to litigate motions for sanctions based upon claims of spoliation.[112] In *Metropolitan Opera Association v. Local 100, Hotel Employees & Restaurant Employees International Union*, the court stated:

> [C]ounsel (1) never gave adequate instructions to their clients about the clients' overall discovery obligations, [including] what constitutes a 'document' . . . ; (2) knew the Union to have no document retention or filing systems and yet never implemented a systematic procedure for document production or for retention of documents, including electronic documents; (3) delegated document production to a layperson who . . . was not instructed by counsel[] that a document included a draft or other non-identical copy, a computer file and an e-mail; . . . and (5) . .

[110] A company does not have to save every document it generates. In fact, superfluous materials need not be kept, but a streamlined system of document retention is unquestionably necessary. Any policy, however, must take into consideration the duty to retain electronic documents if one believes that litigation is imminent or if a lawsuit has been filed.

[111] Metro. Opera Ass'n v. Local 100, Hotel Employees & Restaurant Employees International Union, 212 F.R.D. 178, 231 (S.D.N.Y. 2003).

[112] *E.g.*, Danis v. USN Communications, 53 Fed. R. Serv. 3d (West) 828 (N.D. Ill. 2000); GTFM, Inc. v. Wal Mart Stores, 49 Fed. R. Serv. 3d (West) 219 (S.D.N.Y. 2000).

> . failed to ask important witnesses for documents until the night before their depositions and, instead, made repeated, baseless representations that all documents had been produced.[113]

[53] Both litigation and the pervasiveness of electronically created and stored information are realities that need to be anticipated and addressed. Employees need to be educated to be mindful of the contents of all electronic documents – especially, but not exclusively, e-mail, text messaging, and other seemingly "informal" means of communication. Systemic controls need to be implemented to enforce document retention and information policies with respect to electronic information. Technology needs to be chosen that facilitates control, retrieval and appropriate destruction of electronic information.

[54] Thomas Y. Allman, an attorney who drafted California's proposed model rules for e-discovery, proffered the following procedures that companies could establish in order to ensure that they are properly protected in case they should become obligated to respond to an electronic discovery request:[114]

- Establish a formal policy which requires each corporate employee to manage business records, regardless of what form the records take, that he creates or maintains in his or her ordinary course of business and make each person cognizant that his or her responsibilities include retaining records of business activity.

- Work with individual business units to develop practices and customs, designed for their business needs, that identify the business records they need to retain.

- Develop presumptive limits on retention of e-mails that are not to be saved as business records and establish communications policies that promote the appropriate use of e-mail and other company-owned systems.

---

[113] *Metro. Opera Ass'n*, 212 F.R.D. at 222.

[114] Thomas Y. Allman, *Back-up Tapes, Best Practices and Rule Amendments*, *at* http://californiadiscovery.findlaw.com/proposed_el_disco_rules.htm (July 21, 2002).

- Eliminate unnecessary retention of backup tapes and deny routine access to back-up tapes for reasons other than crisis reconstruction.

- Establish procedures to identify and notify individuals and business units of the need to preserve electronic and other records which may be relevant for threatened or pending litigation.

- Publicize policies and procedures for preserving potential evidence when threatened with litigation. Also, train lawyers and business people on when and how to preserve the information for which they are responsible.[115]

D. *Marshall Appropriate Resources to Assist with Production*.

[55] Companies should not skimp when allocating resources toward a document retention plan. As with emerging technology, it is important to do it correctly the first time. Any person who has lost work due to a computer crash knows that once information is lost or destroyed, there often is no going back. Use of proper resources can help minimize the costs and maximize the benefit of information technology in litigation.

[56] Even more importantly, though, recent case law makes it clear that courts will force the production of electronically stored data and materials. In planning their budgets, companies may want to take into account not only the cost of maintaining and storing electronic data but also the cost of retrieving and producing it. It can be very costly to produce electronic files, duplicate hard drives, restore back up tapes, and resurrect outdated software. Companies cannot expect that this cost will automatically be shifted to the party requesting the electronic data. Accordingly, businesses with appropriate systems can reduce the "pain" necessary to meet the obligations of doing and protecting business in an electronic age.

V. CONCLUSION

[57] Electronic documents now form the basis of many internal and external business transactions. Companies are routinely communicating with their employees via electronic transmission. Oftentimes the only

[115] *Id.*

record companies have of their business decisions, results, and strategies are maintained in electronic form. Accordingly, it is imperative that a company put into place the protocols necessary to support the confidentiality, integrity, and availability of its electronic documents.

[58] To be properly prepared in the electronic age, businesses must have an effective document retention policy in place that addresses electronically stored information, data, and materials. They must also have company-wide policies for dealing with that information, especially policies relating to the storing of e-mail communications. It is important that those policies are well known and properly communicated to all employees so that those responsible for maintaining and storing the records can have the information required to perfect the task.

[59] It is not only important that the protocols are in place, but it is imperative that the documents maintained withstand judicial scrutiny. For records to be admissible in court, companies must have the resources available to show a chain of custody of the electronic data. They must have the personnel in place who know the company's computer system and can explain the inner-workings of the system in a concise, understandable, and informed manner. Accordingly, senior management must make decisions as to whether the maintenance of the company's records and computer system remains an in-house function headed up by a company employee or whether it is in the company's better interest to outsource the work to a third party service provider who deals solely with maintenance of electronic records.

[60] To survive in an electronic world, corporations must be aware that risk management is one of their most important tasks. One of the foremost concerns of risk management is the company's information technology system. Companies must strive to insure that their records are not only admissible but also of indisputably flawless value. Therefore, senior management should consider allocating the time, money, and efforts usually directed toward new business strategies or product develop to their information technology systems – and make sure that those systems are updated, organized, and working properly in order to make themselves ready and properly armed to conduct business in the electronic age.