



The International Council of Shopping Centers

Retail Law Strategist

Vol. 7, Issue 5 – THE PROBLEM-SOLVING TOOL FOR RETAIL LAW – May 2007

“E-DISCOVERY”: MODEST RULES PORTEND DRAMATIC PROBLEMS—Part 1

ROBERT A. MACHSON

Robert Machson & Associates, LLC
New York, NY

Those of us who are preoccupied with leases, easements, exclusives and the like may not be aware that new changes to the Federal Rules of Civil Procedure might cost your client millions and change the outcome of any litigation in which he or she is involved. Of course, if you are sure that your client will never sue or be sued, then this topic will be of little interest.

As of Dec. 1, 2006, new amendments to the Federal Rules of Civil Procedure mark a sea-change in the way litigation is conducted. These are new amendments concerning “e-discovery,” which require businesses immediately to assess the ways in which they create, use, transmit and store all of their electronic information. (While this article concerns the federal rules, these rules generally are followed by state courts and, therefore, their impact will be virtually universal.)

As the name suggests, “e-discovery” means that everything created and kept in this new age of virtual mail, data and record-keeping is subject to disclosure in litigation. The amendments are recognition, not only of this new technology—i.e., the software—but also of the exponentially greater volume of data that has been, and can be, stored. Even modest organizations now have the capacity to archive information in “terabytes,” each of which can store the equivalent of 500 million typewritten pages of plain text and tens of millions of e-mail messages monthly.

Compared to the days when corporations and attorneys simply had to worry about documents stored in boxes, the potential of tens of millions of documents stored in untold numbers of accessible and inaccessible formats presents problems that scholars, judges and attorneys have only begun to consider.

This article is divided into three parts that will appear in future RLS issues. It begins with a general (though by no means exhaustive) review of the new amendments; Part 2 examines some of the recent decisions concerning “e-discovery”; and Part 3 provides some suggestions to address the challenges presented by electronically stored information.

Part 1: The “Modest” Changes to the Federal Rules

The drafters of the new amendments (“the Committee”) described their changes as “modest.” However, this might be misleading. These amendments, and the judicial decisions that preceded them, are likely to have a profound effect on how companies conduct their business and how

disputes will be resolved.

The most obvious change to the rules is found in Rule 26, which requires the “initial disclosure” of “electronically stored information.” This makes it clear that each party has an initial burden at the commencement of any litigation, not just during discovery, to disclose all potential documents, including those stored electronically. The Committee was aware that this would include a seemingly endless amount of information that could not be readily accessed, including e-mails and Excel charts, drafts of documents and archived documents, and documents stored in software programs that may no longer exist (“legacy data”). Nevertheless, they chose to impose this obligation—however likely it was to increase a party’s burden.

In order to mitigate the burden presented by this initial obligation, the Committee added a new provision [Rule 26(b)(2)(B)], which relieves a party from producing electronically stored information “that the party identifies as not reasonably accessible because of undue burden or cost.” Examples of inaccessible sources might include “archival data,” legacy data, and deleted or fragmented data. (An extremely useful glossary of e-discovery terms can be found at www.thesedonaconference.org/content/miscFiles/publications_html.) Nevertheless, because the Committee has made clear that all “potentially responsive” information must be disclosed, it is likely that the party receiving this information will want to know more about what is contained in this “inaccessible” data, and may move to compel its discovery.

In that event, the rule requires that the party from whom the discovery is sought must first “show that the information is not reasonably accessible.” The Committee Notes make clear that the responding party cannot simply state that the information is difficult and expensive to access. It must identify by “category or type” the sources containing the potentially responsive information that is not being searched or produced. In practical terms, this means that the party withholding production needs to identify not only the subject matter of what is being withheld, but what form it is in and the cost of its identification, retrieval and (if necessary) recovery. See *Hopson v. Mayor and City Council of Baltimore*, 232 F.R.D. 228 (D. Maryland 2005). By itself, this process may represent a significant expense.

In addition, the Amended Rules touch upon, but some would argue fail to resolve, another difficult problem that becomes apparent when a party is required to disclose large amounts of data that have long been stored and forgotten. The problem is that, among potentially hundreds of thousands (or millions) of pages of “documents,”

many may be protected as “work product” or may be privileged. As the Committee reported in its commentary to Rule 26(f):

Production may be sought of information automatically included in electronic files but not apparent to the creator or to readers. Computer files may retain draft language, editorial comments, and other deleted matter (sometimes referred to as “embedded data” or “embedded edits”) in an electronic file but not make them apparent to the reader.

Rule 26(b)(5)(B) sets up a procedure by which a party that has inadvertently produced material that may be protected can notify the receiving party and ask for its return. The party receiving the notification must then return, sequester or destroy the information.

The difficulty with this new provision is that it is not substantive (and the Committee purposely avoided any changes to the substantive rules of privilege). In other words, despite the notification and retrieval procedure, the protection or privilege may nevertheless be lost by the disclosure. The Committee thus suggests that parties producing large amounts of data agree before the production to return any protected or privileged information without waiver.

Alternatively, the producing party may permit a review of all the materials, subject to its ability to screen and protect those documents selected by the receiving party. These agreements have been given the descriptive monikers of “clawback” and “quick peek.” (It is important to note that any protections afforded by these claw-back and quick peek agreements may not be enforceable against claims of waiver by third parties.) The time for the parties to discuss and enter into these agreements is prior to the pretrial conference required under Rule 16, which has been amended to encourage parties to enter into agreements for the disclosure of electronically stored information and the assertion of claims of protection or privilege. See Rules 16(b) (5) and (6). Unfortunately, the case law discussed in Part 2 makes it clear that, notwithstanding these agreements, there is still no guaranteed protection for inadvertently disclosed material.

Part 2 will discuss the evolving case law; Part 3 will address avoiding and anticipating e-discovery problems. ■

ROBERT MACHSON has represented large chain retailers for over 15 years. He is a member of the Board of Editors of the Retail Law Strategist and a Director of the National Retail Tenants Association. Bob can be reached at RM@RetailLaw.com



“E-DISCOVERY”: MODEST RULES PORTEND DRAMATIC PROBLEMS— Parts 2 and 3

ROBERT MACHSON

Robert Machson & Associates, LLC
New York, NY

Part 1 was a general review of the new e-discovery amendments

Part 2: The Evolving Case Law

Not surprisingly, there is little case law to answer the questions created by the new e-discovery amendments and the changing technology. *Universal Service Fund Telephone Billing Practices Litigation*, 232 F.R.D. 669, 673-74 (D. Kan. 2005) [“electronic discovery is a rapidly evolving area in which litigants (and judges) often have little or conflicting guidance.”]. Notwithstanding the absence of guidance, mistakes—even those made in utter good faith—may have severe repercussions.

Preservation of Electronically Stored Information

Given the amount of information that can be electronically stored and the prevalence of routine policies that result in the deletion or archiving of information, the question of when, and under what circumstances, electronically stored information can be destroyed will assume increasing importance. While parties have always been prohibited from destroying documents that they know (or have reason to believe) may be subject to discovery in litigation, what is a party’s obligation with respect to documents that may or may not be relevant, but may be filed or archived along with a great deal more information that will not be relevant?

Needless to say, “[d]iscovery of electronic data presents unique problems that do not exist for the discovery of paper documents.” *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 214 (S.D.N.Y. 2003) (“*Zubulake II*”). Principle among these unique problems is the degree to which a party must preserve electronically stored files, including its e-mails. (Given their ubiquitous role in *intra* and *inter* office communications and the likelihood that they

may contain the most unguarded information, e-mails are the first target of discovery demands.)

In partial response to this dilemma, Rule 37(f) was added to provide a “safe harbor” for the destruction of electronically stored information, prohibiting a court absent “exceptional circumstances,” from imposing sanctions for information lost “as a result of the routine, good faith operation of an electronic information system.” Notwithstanding this new rule, it is clear that there is no *carte blanche* to destroy information at any time, even as a result of routine maintenance.

Trigger Dates

A party’s duty to preserve electronic evidence (and most other evidence) is generally defined by the “trigger date.” An obvious trigger date is the commencement of litigation, though it may also be some other, preceding, event. *See E-Trade Securities LLC v. Deutsche Bank AG*, 230 F.R.D. 582, 589 (D. Minn. 2005) (a party may be required to preserve evidence before litigation is commenced, when it “clearly knew about the potential for litigation”). Thus, an organization that frequently deletes and purges electronic files subjects itself to sizeable risk if it fails to take adequate steps to preserve data. *See Broccoli v. Echostar Communications Corp.*, 229 F.R.D. 506 (D. Maryland 2005) (failure to issue company-wide instruction suspending data destruction policy deleting documents within 30 days and e-mails within 21 days subjected company to severe sanction).

A party has no duty to preserve evidence before the trigger date. It does have a duty to preserve evidence after the trigger date, even if the evidence was destroyed as a result of “routine maintenance.” *Clark Const. Group, Inc. v. City of Memphis*, 229 F.R.D. 131 (W.D. Tenn. 2005). The failure of a party to insure that documents are not “routinely” destroyed may subject it to severe sanctions, including an adverse inference jury instruction (as to the information

that was destroyed) and default. *Id.*

Thus, it is imperative that a party with reason to believe it may be subject to litigation put a “hold” on all of its electronic retrieval—not only so that documents and e-mails are preserved, but also so that they are preserved in a manner in which they can be readily produced.

Privilege and Waiver

Doubtless, the potential production of “megabits” of information, consisting—e.g., of untold numbers of relevant and irrelevant e-mails, documents and spreadsheets—raises the specter of inadvertent waiver of work product protection and attorney-client privilege.

As noted in Part 1, the Amended Rules permit and seemingly encourage parties to enter into voluntary agreements to safeguard the inadvertent production of this material. The laudable goal is to reduce the enormous cost that even minimal review might entail. Yet, as noted by at least one court, the Committee failed to come up with a solution, noting that “no prudent party would agree to follow the procedures recommended in the proposed rule.” *Hopson, supra*, 232 F.R.D. at 234.

Unfortunately, there is no consistent rule of law governing the inadvertent production of protected information. Instead, various jurisdictions have adopted different standards for determining when a waiver takes place. These have been sorted into three general categories. The first, a “strict accountability” standard, almost always finds waiver, even if the production was inadvertent; the second, a more lenient standard, finds waiver only if it was knowing or caused by gross negligence; and the third, which adopts a balancing test, requires the court to make a case-by-case determination to see whether the conduct (waiver) was excusable.

Nevertheless, one court, after an exhaustive and enlightening review of each of these standards, warns that “even in those jurisdictions that have adopted the more lenient ‘balancing test,’ the producing party still must show



The International Council of Shopping Centers

Retail Law Strategist

Vol. 7, Issue 5 – THE PROBLEM-SOLVING TOOL FOR RETAIL LAW – June 2007

that reasonable measures were taken to screen for privileged information. The better approach is to assume that complete pre-production privilege review is required, unless it can be demonstrated with particularity that it would be unduly burdensome or expensive to do so.” *Hopson, supra*, 232 F.R.D. at 244.

The expense of review is compounded by the difficulties encountered in “logging” protected and privileged documents. This is the process of identifying the documents that have been withheld in order to permit the requesting party or a court to determine whether the privilege was appropriately asserted. Courts have already expressed concern that relevant, non-protected information could be buried through “stealth” disclosure among protected material. For that reason, one court ordered the producing party in a large commercial litigation to log each e-mail in a number of long e-mail “stands” separately and fully, even though it recognized that this would pose “a very significant drawback to modern commercial litigation.” *Universal Service Fund Telephone Billing Practices Litigation*, 232 F.R.D. 669, 673-74 (D. Kan. 2005).

Cost of Producing Archived Materials

Another rapidly emerging concern is determining which party should bear the expense of restoring data that is not immediately accessible. Given that the costs may exceed several hundred thousand dollars, see *Quinby v. WestLB, AG*, 2006 WL 2597900 (S.D.N.Y. Sept. 5, 2006) (in an employment discrimination case, defendants claimed that plaintiff’s demand to retrieve archived information would cost \$226,266), the decision as to which party will bear the burden of this expense may have a significant impact upon the outcome of a case. At the risk of repetition, the relevant case law is sparse.

The few courts which have examined this issue are in agreement that only the costs associated with producing data from inaccessible formats can be considered for cost shifting. *Zubulake v. UBS Warburg, LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003) (“*Zubulake I*”). Thus, it would not be considered an

“undue burden” for the responding party to retrieve data that is kept in a readily usable format. However, if a party “creates its own burden or expense by converting into an inaccessible format data that it should have reasonably foreseen would be discoverable material at a time when it should have anticipated litigation, then it should not be entitled to shift the costs of restoring and searching the data.” *Quinby, supra*, Slip Op. at 9. Thus, the importance of the trigger date arises again.

Nevertheless, the trigger date does not create an iron-clad rule as to when the cost of restoring data should be shifted from the producing to the requesting party. Courts have established a number of factors to be weighed in determining whether cost shifting is appropriate. See *Zubulake I*, *supra*, 217 F.R.D. at 322 and *Quinby*, Slip Op. at 11-12. Additional factors are the degree to which the inaccessible data is likely to contain relevant discovery (and the degree to which the requesting party has tailored its demand) and the relative costs, including the amount in controversy versus the cost of production.

Part 3: Avoiding and Anticipating E-Discovery Problems

At the very least, the astronomical costs associated with e-discovery should compel a re-thinking of the ways in which business maintains and stores data. Gone are the days when a well-meaning policy to “keep everything” makes much sense.

The difficulty of protecting one’s self or organization is compounded by the fact that, until recently, most of us ignored these e-discovery issues. Therefore, little thought was given to the way documents were either deleted or archived. The Amended Rules and the accompanying case law put everyone on notice that past practice needs to change . . . and fast.

Perhaps the first thing to be examined is the way in which data is stored. For example, many corporations continue to store data on outdated tapes that are unlabeled and difficult, if not impossible to access (at anything other than astronomical cost). To the extent

this data is not being saved under a well-conceived document retention policy or in reasonable anticipation of litigation, it may be prudent to consider their destruction now.

Likewise, companies should consider the ways in which they now retain and store data, including the frequency with which documents, including e-mails, are archived or deleted. In addition, even though archived data may be “inaccessible” under the new rules, the data should be stored in such a way that it will not be unduly expensive to retrieve and catalog.

At the same time, the procedures by which litigation “holds” are initiated and employees are alerted should be reviewed and disseminated. The failure of a seemingly “uninvolved” employee to save data may have severe consequences.

Companies also may need to engage in “e-education.” Businesses should take the time to train their employees, including their senior management, about what should and should not be saved, including drafts of documents (which may contain embedded data and notes), Excel chart(s), etc. Needless to say, e-mail belongs in a category by itself; because it is relatively new, is used by virtually everyone, and is pervasive in homes and offices; the degree to which e-mail creates litigation nightmares is only now becoming apparent. Litigators have quickly become wise to the fact that the best source of “smoking guns” is the casually conceived, quickly “clicked” message that, if composed on paper, would never have been sent.

As promised, this article began with some dry new rules and ended with some alarming warnings. To the extent that this is viewed as a cautionary tale, it has achieved its purpose. ■

ROBERT MACHSON has represented large chain retailers for over 15 years. He is a member of the Board of Editors of the Retail Law Strategist and a Director of the National Retail Tenants Association. Bob can be reached at RM@RetailLaw.com.