EIGHT-MINUTE
ELECTRONIC DISCOVERY

Adam T. Klein, Esq.
Tarik F. Ajami, Esq.
Douglas C. James, Esq.
Rachel Wilhelm
Outten & Golden LLP
3 Park Avenue 29th Floor
New York, New York 10016

Technophobes, relax: electronic discovery is, at its core, just discovery. And being discovery, it is fundamentally the process of locating, reviewing, and producing materials that are not privileged and that are reasonably likely to lead to evidence admissible at trial. Fed. R. Civ. P. 26(b)(1). But today, virtually every document on the planet is generated and stored in some kind of digital format. The practical effect of this is that plaintiffs and defendants alike are, perhaps unknowingly, sitting atop a mountain of invisible documents, many of which may well be discoverable in the event of litigation.

So technophobes, be nervous as well. If you haven't already, it is incumbent upon you to vanquish your inner Luddite and familiarize yourself with how your discovery obligations and opportunities have changed in recent years.

Good News: Every Case Should Implicate Electronic Discovery.

Attorneys must enter every case assuming that electronic discovery will be involved. Indeed, electronic discovery may often be the key to success or failure, given a few of its salient characteristics.

First, and perhaps most obviously, data or other materials stored electronically are often physically easier to store, produce, review, and use. Reams of "paper" can be

stored on-site, retrieved with a few keystrokes, and produced on a single ROM device such as a DVD. Massive amounts of materials can be searched for concepts or key words. Archived data – such as personnel databases or payroll records – can be subjected to all sorts of analyses, from simple spreadsheet tabulations to complex econometric modeling.

Second, electronic materials are often highly probative. Databases, as mentioned above, contain easily digested and massaged fields of data that, in the aggregate, may point conclusively to liability or exoneration. Drafts of documents and other abortive materials that in earlier years may have been shredded or destroyed are routinely preserved. Email, for whatever sociological reason, lends itself to a sort of frank and free-flowing banter that has all but vanished even from the shop floor.

Lastly, electronic materials are wonderfully – or frustratingly, depending on your vantage point – durable, often resisting even the most determined attempts to destroy it. It can linger seemingly forever in the forms such as back-up tapes, archives, removable media, erased and fragmented data, metadata, and other such spectral forms.

Meta-What?

One of the most effective ways to arm oneself for the age of electronic discovery is to learn a few basic terms and throw them around wildly whenever litigation is even hinted at.

The first term every lawyer needs to know is "Zubulake," as in *Zubulake v. UBS Warburg, LLC*, the case that spawned a thousand (or five) extremely influential opinions

on electronic discovery.[1] In the first of the series, the aptly named *Zubulake I*, Judge Scheindlin offered a handy glossary of the types of electronic data generally encountered in litigation. *Zubulake v. UBS Warburg* LLC, 217 F.R.D. 309, 318-19 (S.D.N.Y. 2003). Learning these few terms puts one well on the way to facility with electronic discovery issues:

Active, online data: Data generally stored by magnetic disk and "used in the very active stages of an electronic record's life . . . . Examples of online data include hard drives." *Id.* at 318.

Near-line data: Typically a robotic storage device "that houses removable media, uses robotic arms to access the media, and uses multiple read/write devices to store and retrieve records . . . . Examples include optical disks." *Id.* at 318-19

Offline storage/archives: Removable optical disk or magnetic tape media, which can be labeled and stored in a shelf or rack–"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 speed may be minutes, hours, or even days, depending on the access-effectiveness of the storage facility. The principled difference between nearline data and offline data is that offline data lacks 'the coordinated control of an intelligent disk subsystem,' and is, in the lingo, JBOD ("Just a Bunch of Disks")." *Id.* at 319.

Backup tape drives: Reads data and writes in onto a tape, much like a tape recorder. Tape drives have a wide range of capacity and widely varying transfer speeds.

[1] For those seeking extra credit, it is pronounced "ZOO-buh-lake," not "Zoo-boo-LAH-kay."

"The disadvantage of tape drives is that they are sequential-access devices, [resulting in the fact that] the data on a backup tape are not organized for retrieval of individual documents or files . . . . Backup tapes also typically employ some sort 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[s] governing data compression." *Id.*

Erased, fragmented or damaged data: "When a file is 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 placed throughout the disk. Such broken-up files are said to be 'fragmented,' and along with damaged and erased data can only be accessed after significant processing." *Id.* Another term frequently encountered in this context is "*metadata*." Metadata, to oversimplify, are data about data. "'Metadata,' which also is referred to as 'data about data,' is a relational database that contains information about the data located in a data warehouse." *MicroStrategy Inc. v. Li*, 601 S.E.2d 580, 583 (Va. 2004). In digestible language, and for purposes of this discussion, metadata refers to data embedded in a document that describes the document and its contents. Metadata usually "include[s] the author [or authors] of the document, the dates and authors of modifications of the document, when and by whom a document was reviewed, and when the document was last accessed" and by whom, among other potentially illuminating information. *In re Telxon Corp. Sec. Litig.*, No. 5:98CV2876, 2004 WL 3192729, at *16 (N.D. Ohio July 16, 2004). For obvious reasons, metadata can provide critical support to a party's claims

or defenses. However, one may access metadata only from a document in its electronic form – it is not printed on hard copies and is typically invisible in screen shots of a document – highlighting the importance of conducting aggressive and thorough electronic discovery. *See Zenith Elec. Corp. v. WH-TV Broad. Corp.*, No. 01 C 4366, 2004 WL 1631676, at *7 (N.D. Ill. July 19 2004).

Getting the Electronic House in Order.

So if nearly every case likely implicates electronic discovery, every lawyer has electronic obligations.

As with any other kind of document, a party is obligated to retain and preserve electronic documents once it is given notice that those documents are relevant to litigation. *See, e.g., Kronisch v. U.S.*, 150 F.3d 112, 126 (2d Cir. 1998). This isn't limited to the moment the action gets filed; rather, once any party learns it has or may have information relevant to the case, it is under a duty to protect that information from spoliation. *Id.*

Of particular concern for corporations, this obligation requires or should require that the corporation have some sort of document retention policy in place. This policy should allow the corporation to (a) define what data exists; (b) determine what among it is relevant to the actual or potential claim or defense; (c) locate the data and preserve it; (d) review it; and (e) in the case of actual litigation, produce it where required.

It is not merely enough for the lawyer representing a corporation to speak about methods of data storage and retention with her client's information technology personnel. Rather, if Judge Scheindlin's dictate in "*Zubulake V*" is followed, the lawyer will discuss the matter with each "key player" witness as well. *Zubulake v. UBS Warburg LLC*, No.

02 Civ. 1243, 2004 WL 1620866, at*8 (S.D.N.Y. July 20, 2004). This enables the lawyer to ensure that she has learned about alternate repositories of data, such as a witness's PDA, BlackBerry, home computer, or floppy disks (if those even exist anymore) rattling around in a briefcase.

Once the lawyer determines the extent and location(s) of discoverable electronic materials, she and her client should take steps to ensure that the material is not destroyed. If the client is a large organization, they may run afoul of the company's usual document retention policy, under which stale data is periodically wiped from the company's storage devices. In such cases, the lawyer should advise her client to at least institute a so-called "litigation hold" to temporarily suspend these practices and preserve data from destruction, and at least check in from time to time.

The far better practice would be to order "mirroring" of relevant storage devices. This practice effectively takes and saves a snapshot of data on the device at a given moment in time, preserving it in that state for future review and production.

From a plaintiffs' perspective, it is crucial to be aware that these automated procedures are at quietly work at most large defendants, routinely shredding massive amounts of data. Weeks or even months can pass between the lawyer's initial intake and the day she files her complaint, and each day that passes can mark the destruction of more and more evidence. It therefore behooves the careful plaintiffs' lawyer to craft and send a thorough and directed "spoliation letter" to a potential defendant as soon as discretion allows. The spoliation letter should serve to put the potential defendant on notice of the existence and nature of the potential claim, and at least generally describe the types of documents that should be preserved. If done early and properly, this should

place the onus squarely on the potential defendant's lawyers to preserve critical documents.

Document Preservation: The Problem That's Already Yours.

None of this is new. Independent of her obligations under the Federal Rules, a lawyer has an ethical obligation pursuant to Model Rule 3.4(a) of the ABA's Model Rules of Professional Conduct to prevent spoliation or destruction of data and other materials. That Rule states that an attorney shall not:

> (a) unlawfully obstruct another party's access to evidence or unlawfully alter, destroy or conceal a document or other material having potential evidentiary value. A lawyer shall not counsel or assist another person to do any such act[.]

As set forth in the Comments to Rule 3.4(a), "many jurisdictions [make] it an offense to destroy material for purpose of impairing its availability in a pending proceeding *or one whose commencement can be foreseen*. Comment 2 (emphasis added). Spoliation letters, litigation holds, and filed complaints aside, attorneys have a freestanding, independent ethical obligation to not assist in any way in the destruction or alteration of electronic documents with "potential evidentiary value." Rule 3.4(a).

That's Going to Hurt in the Morning.

In fact, lawyers allow the spoliation on their watch of relevant evidence – electronic or otherwise – at their peril. While perhaps an outlier, *Metro. Opera Assoc., Inc. v. Local 100, HERE Int'l Union*, 212 F.R.D. 178 (S.D.N.Y. 2003) should fill any lawyer with some amount of dread. In that case, the court issued the most severe sanction possible against a defendant for its noncompliance during discovery: she entered judgment in favor of the plaintiff on all causes of action. *Id.*

If *Met Opera* is to be followed, counsel may not simply content herself with issuing directions to her client about document preservation and production, and checking from time to time. *Met Opera* seems to require that counsel supervise and *conduct* document and electronic production herself: "nothing . . . indicated that a thorough search had been made or that any document production had been supervised or conducted by an attorney." *Id.* at 189. *Met Opera* suggests that is indeed sanctionable for an attorney to simply instruct and inform the client as to what needs to be turned over. *See, e.g.*, *Id.* at 185 ("[the research director] is not a lawyer, and there is no indication that [the president] is a lawyer"); *Id.* at 211 (defendant's office manager had no recollection of a lawyer asking her to look for certain documents); *Id.* at 213 (defendant's attorney did not personally search files "[d]espite [plaintiffs'] counsel's constant clamoring for a complete file search supervised by an attorney").

While *Met Opera* may represent an extreme case, it is still a cautionary tale. If we are to learn a lesson, it is that lawyers should be proactive and serious about their duties to preserve and produce electronic information and other discovery materials.

Who's Gonna Pay for All This?

As noted earlier, one advantage of electronic discovery is that it can often be easier and cheaper than producing paper files. But this isn't always the case.

For example, as discussed earlier, "document retention" policies may have already chewed through and deleted reams of relevant electronic materials. Witnesses may have deleted damaging emails from their hard drives. In these circumstances, it is incumbent upon an attorney to learn in what forms those documents may still exist – on backups, copied onto offline storage devices, or as fragments. Especially where data are

relatively inaccessible, as is the case with backed up or deleted data, the costs of production may begin to skyrocket.

The general presumption in federal discovery, of course, is that the producing party bears the costs of production. *Zubulake v. UBS Warburg LLC ("Zubulake III")*, 216 F.R.D. 280, 283 (S.D.N.Y. 2003). However, there are exceptions, at least according to the *Zubulake* court. Regarding materials on back-up tapes or deleted and/or fragmented materials that must be restored, a court may consider ignoring the presumption and shifting all or part of the costs of production to the requesting party. *Zubulake I*, 217 F.R.D. at 324 ("A court should only consider cost-shifting when electronic data is relatively inaccessible, such as in backup tapes."). Cautioning that "close calls should be resolved in favor of the presumption," the court set forth the following factors to consider when cost-shifting is requested:

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

Note that these factors are not equal; the court presented them descending order of importance. *Id.* at 322.

The first two factors, weighing "marginal utility," are, in the *Zubulake* court's view, most important:

> The more likely it is that the backup tape contains information that is relevant to a claim or defense, the fairer it is that the [responding party] search at

> its own expense. The less likely it is, the more unjust it would be to make the [responding party] search at its own expense. The difference is "at the margin."

Id. at 323 (quoting *McPeek v. Ashcroft*, 202 F.R.D. 31, 34 (D.D.C. 2001)). Factors three through five "[address]cost issues: 'How expensive will this production be?' and, "Who can handle that expense?'" *Zubulake I*, 217 F.R.D. at 323.

Regarding the sixth factor, "the importance of the litigation itself . . . will only rarely come into play. But where it does, this factor has the potential to predominate over the others." *Id.* Where cases have a "potential for broad public impact," such as "class actions [and] so-called 'impact' or social reform litigation, or cases implicating important legal or constitutional questions," "public policy weighs heavily in favor of permitting extensive discovery." *Id.* at 321.

The last factor is the least important. Indeed, one can presume that "the response to a discovery request generally benefits the requesting party. But in the unusual case where production will also provide a tangible or strategic benefit to the responding party, that fact may weigh against shifting costs." *Id.* at 323.

Of course, the problem remains balancing the likelihood that an involved restoration will yield relevant information against the costs of such restoration. *Zubulake* resolved this conflict by adopting a sampling approach – *i.e.*, "[r]equiring the responding party to restore and produce responsive documents from a small sample of backup tapes [to] inform the cost-shifting analysis . . ." *Id.* at 324. Once that sample is produced, "the entire cost-shifting analysis can be grounded in fact rather than guesswork." *Id.*

The Zubulake court recognized and sought to bring some balance to the reality of electronic production. The court recognized that electronic production can, on limited

occasions, be a massive and expensive proposition; nevertheless, the court took great pains to reaffirm that cost-shifting should be the remote exception and not the rule.

The More Things Change . . . .

If electronic discovery is just discovery of materials that in bygone eras would by and large have been stored in hard-copy format, it is probably true that few if any changes to the Federal Rules of Civil Procedure (or its analogues) are really needed. Nevertheless, adaptability and the pursuit of clarity are never bad things.

In that spirit, the Advisory Committee on the Federal Rules of Civil Procedure has undertaken some suggested revisions to the Rules to reflect, in part, lessons learned from the unique struggles sometimes created by electronic discovery. These changes are long view, and are not anticipated to take place before early 2007. Not all of these changes are limited to or specifically address electronic discovery. Without delving into exhaustive detail, some of the proposals are outlined and discussed below:

Rule 26(f) – Initial Party Conferences: The proposed amendments would place the onus on the parties to, right up front, discuss (a) preservation of materials, (b) the format in which they are to be produced, and (c) the right or ability to protect privileged material *after* production. These changes are more of a modernization of the Rules to reflect practices that have come into vogue – such as agreements protecting inadvertent or even intentional disclosure of privileged materials – but they do bear in certain respects on electronic issues. Of particular interest is the suggestion that requesting parties are entitled to specify or at least urge that electronic materials be produced in a particular format.

Rule 16(b) – Initial Court Conference: In many respects a companion to the changes to Rule 26(f), these changes would add some straightforward and frankly fairly vanilla items to the standard preliminary conference's agenda: (a) "provisions for disclosure or discovery of electronically stored information," and (b) "adoption of the parties' agreement for protection against waiving privilege." This is interesting primarily insofar as it seems to reify the practice of discovery agreements governing waiver of privilege into something like a requirement or expectation.

Rule 26(b)(2) – Accessible Information: This is an important revision that may be the recipe for much delay and added motion practice. The amendment would allow a producing party to object generally that a request seeks "electronically stored information" by claiming that the information is "not reasonably accessible." Upon such a claim, the requesting party may move to compel production of the materials. Only at that point does the producing party bear the burden of actually showing that the information really isn't reasonably accessible. If the producing party succeeds in making its showing, the burden shifts back to the requesting party to show "good cause" for an order requiring production of the materials.

Rule 26(b)(5) – Clawback of Privileged Materials: This change would uniformly protect unintentional (not just inadvertent) production of privileged materials in federal litigation. Such privilege issues move to the fore in the electronic age as massive and speedy "data dumps" can lead more easily to the inadvertent productions this rule change is designed to address. But this change is mostly interesting because it would appear to override rules in many jurisdictions that state that any production of privileged matters, irrespective of intent, shatters the privilege.

Rule 34 – Document Requests: In part, revisions here would extend the inspection and copying provision of the rule to include "test[ing]" and "sampl[ing]" of electronic information. Another key change would allow a requesting party to specify the "form in which electronically stored information is to be produced," and allow a responding party to object to that form. Further, if requests under the proposed revisions do not specify a form, the responding party should produce the electronic material in the form "in which it is ordinarily maintained, or in an electronically searchable form." Whatever the case, the producing party need only produce the materials "in one form."

Rule 37(f) – Safe Harbor from Sanctions: This proposed update would shield parties from sanctions relating to electronically stored information. In particular, courts would be forbidden from entering sanctions under the Federal Rules against a party for destruction of electronic information where the party (a) took reasonable steps to preserve the information after it knew or should have known the material was discoverable; and (b) the information was destroyed by routine operation of the party's automatic information systems and document retention programming. Whether this is a good idea is open to debate. For one thing, the Federal Rules themselves provide for little in the way of discovery-related sanctions, so this tiger may be relatively toothless. Secondly, with the harbor's emphasis on automated operations, the amendment may incentivize parties to set their systems to delete materials even sooner than they might otherwise.

Other changes: conforming changes are also proposed for Form 35, which is the report from the 26(f) planning meeting, and for Rule 45, to bring subpoena rules in line with the changes to Rule 34.

* * *

In sum, while little may have changed in the basic thrust of federal discovery and litigation, the world has changed perceptibly. While attorneys' *obligations* have not been altered in particularly meaningful ways, the means and methods by which one ensures that those obligations are met have shifted with the times. Inasmuch as the practice of law is, on a simplistic level, the enforcement of societal norms and encouragement of reasonable behavior in light of those norms, a lawyer should view it as her duty to keep abreast of changes in the way things work and are done. Evidence and potential evidence is being stored and manipulated in different ways. Lawyers need to know how to dig it up, and how to produce it where required.