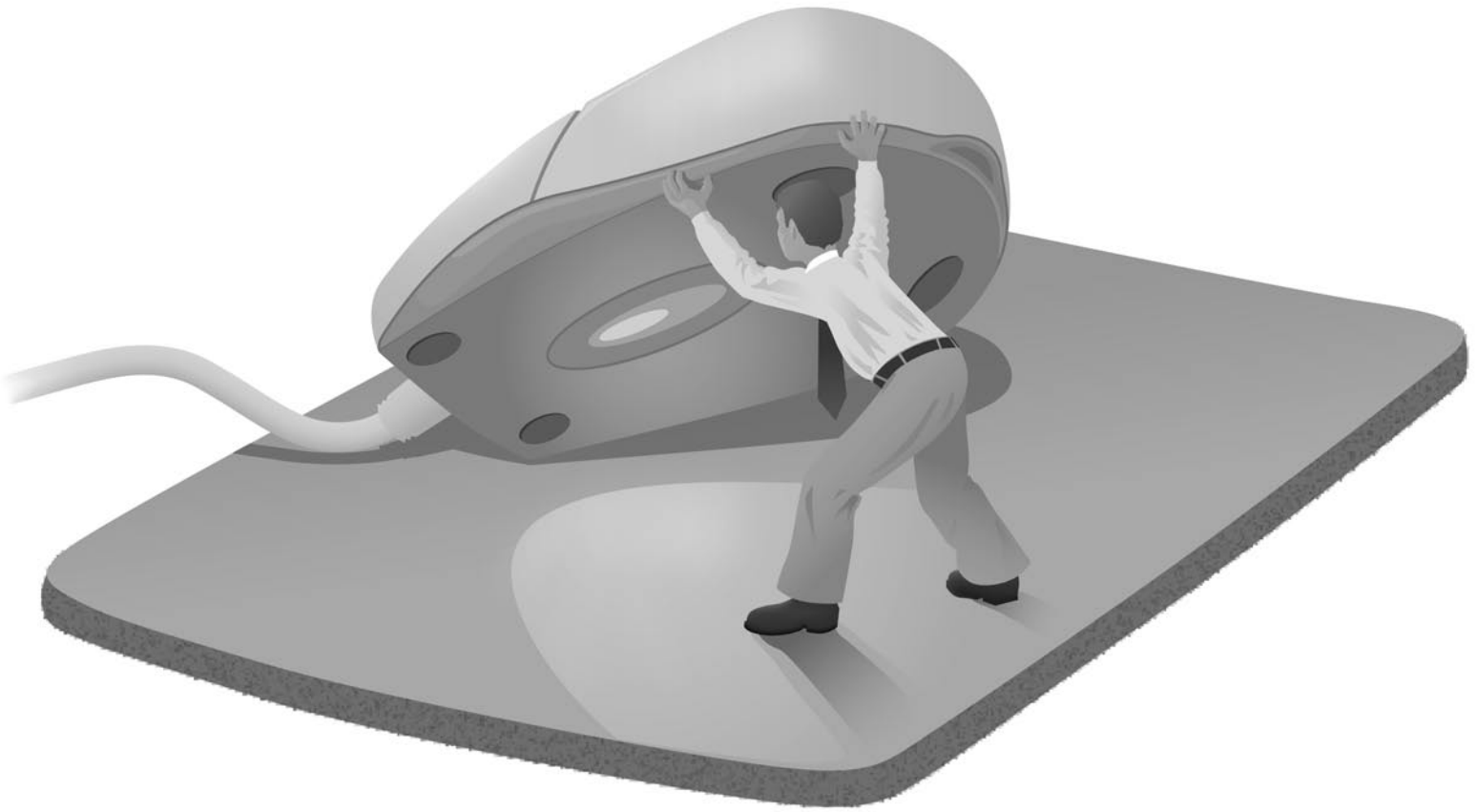

Employment/Civil Rights

Electronic Discovery in employment cases

by
Harris D. Butler, III
Tim Schulte
Rebecca Royals
Blackwell N. Shelley, Jr.

Virtually all employers now keep records in electronic form. These records include email, word processing documents, spreadsheets, time records, building access records, voice mail, faxes and fax logs, and scanned documents. By keeping records in electronic format, employers inadvertently leave electronic fingerprints on every record they touch. In the transition from a paper-based to a digital world, files that employers once kept in central locations have migrated to desktop computers, file servers, removable data storage media like floppy disks and CDs, mobile computers like laptops and PDAs, cell phones, and employees' home computers, all of which contain potentially relevant data. Each of these file-storage points may or may not have been backed up, and the archival backup data may be stored onsite, offsite, or even offshore. Relevant data may also be found on local or foreign internet service providers' networks, such as Yahoo! or AOL.

When businesses ran on paper, they destroyed unnecessary copies of documents in order to preserve finite file storage space. The records that were kept were presumed to be organized in a manner related to the "ordinary course of business." With the advent of cheap digital storage, businesses became less concerned with thrift in preserving documents and disciplined record management largely fell by the wayside. Now, numerous electronic copies of documents are made routinely, distributed widely, and forgotten but not deleted. Most of these records will be irrelevant, some might be privileged, but hidden in the disorganization there may be that elusive and explosive piece of evidence that makes the plaintiff's case.

Not knowing what is hidden in the file, of course, causes counsel for the employer to lose sleep.

The Ghost in the Machine: Electronic records can often provide proof of the employer's state of mind

There are many legally permissible reasons for an adverse employment action such as a demotion, transfer or termination. The only illegal motivations are those that violate state or federal statutory law or which independently constitute common law torts. Successful claims that involve employment discrimination laws – like claims of intentional torts – require the jury to find that the employer intended to discriminate against the employee because of some protected characteristic, such as age, gender, race, national origin, religion, or disability.

For the reasons discussed above, internal email exchanges, draft versions of memos or documents and other electronically maintained data are a gold mine for proof of intent. Not unlike a diary entry,

these are the source data of proof for motive. These records are in pristine form, and unlike an interrogatory response, free of a lawyer's gloss or spin. Moreover, the nature of electronic records – in many cases – allows the record to carry its own history of creation, authorship, and modification. Likewise, the media on which the record is stored can provide dramatic clues as to what was once there but now is gone. In forensic terms, every user interaction with a computer leaves behind data related to the actions carried out. In many cases, being able to prove that a document was deleted or modified, and when the deletion or modification occurred, is better proof of intent than the document itself.

Between a Rock and a Hard Drive: The employer has a duty to preserve the evidence

An employer in a discrimination case has a duty to preserve evidence when the employer is first on notice that the evidence is potentially relevant or reasonably likely to be requested during discovery.¹ With regard to electronic records, however, employers have a special problem. Electronic records are not physically stable. Digital information is easily, often inadvertently, changed, overwritten, or obliterated by everyday use of a computer, whether it is a single desktop computer or a network. Merely starting the computer rewrites files. Opening or modifying a file, adding new data onto a hard disk, or running disk-maintenance software can alter or destroy existing data, without the user's knowledge.

Immediately locating and securing the data is therefore an important task for plaintiff's counsel, as well. At the earliest stages of representation, long before the litigation itself begins, plaintiff's counsel should consider sending a written notice to the employer advising the employer of its duty to keep the records safe. From the plaintiff's perspective, a well-written preservation letter will not only help protect "smoking gun" data, it can also send the clear message to a prospective employer-defendant that the plaintiff will use the discovery phase effectively.

Plaintiff's employment lawyers, as a routine matter, should include in their demand letter to the employer/defendant a request that documents pertinent to the client's employment be preserved.² Establishing the duty early on in the claim eliminates the later debate about when the employer should have anticipated that a claim may be out there and, hence, incurred the duty to preserve data. A preservation letter should include at least the following points:

- A demand that the employer secure all files and records (including emails and other electronically or magnetically preserved records) concerning employee's employment with employer and, if applicable, his or her separation from employment.

- A demand that the employer secure all records and documents concerning the employee's pay and benefits as well as such records for comparable employees.
- In appropriate cases, a demand that the employer secure all records of electronic building access systems.
- Notice to the employer of the intent to access computer network(s) and computer systems and to seek the production of documents in their electronic form and a demand that original electronic data (as opposed to paper copies) be preserved. In appropriate cases, this will include the demand that the employer make forensically sound copies of desktop computer and server hard drives, fax machine memory, voice over IP network messages, and PDAs.
- A demand that notice be given promptly to the person(s) who are responsible for employer's computer network and computer systems and to the person(s) who are responsible for employer's record management program.

If the employee's claim proceeds to litigation, an important early step in the pretrial process is to narrow the focus of discovery. Because an employer's store of electronic records may be immense, the employee's counsel should get some essential background information in order to plan for the material discovery requests to come. The inquiry at this stage is designed to determine who is in charge of the employer's electronic records, how those records are created and maintained, how and when data are backed up and where the backup copies are kept, whether data are encrypted or password protected, whether employees have access to the employer's network from their home computers, and other technical details such as the employer's network and desktop operating system(s), types of server and desktop hardware, types of email, word processing, spreadsheet, and other day-to-day software programs, and any custom-built or proprietary programs that the employer uses.

Drinking From The Firehose: The employee's need to tailor discovery requests carefully

The sheer volume of information that may be responsive to a request for electronic records dictates that counsel for the employee must carefully tailor the requests to the particular case. While the employee's counsel will want a broad scope of discovery, the realities of budget and time constraints should dictate a more narrow search. If at all possible, both sides should try to agree on a search protocol for electronic records, including the sources, key words, names, and date ranges to be searched to avoid disputes over the adequacy of production later.

This initial step is contemplated by the proposed changes to Federal Rules of Civil Procedure 16 and 26(f), which establish a process for the parties and court to address early issues pertaining to the

disclosure and discovery of electronic information. If the case appears to involve significant electronic discovery, these conferences are also opportunities for counsel to discuss the deposition, under Rule 30(b)(6), of the employer's electronic records custodian or information technology manager.

If, at this stage, the electronic discovery appears likely to require actual physical inspection of the employer's computer system, the parties should also attempt to agree on a neutral data forensics expert to act as an officer of the court to conduct the inspection.

Judicially recognized categories of electronic records

The U.S. District Court for the Southern District of New York, in *Zubulake v. UBS Warburg LLC* (*Zubulake I*), 217 F.R.D. 309, 318-320 (S.D.N.Y. 2003), broke down electronic data into five categories, based on the media on which they were stored and organized according to the speed with which the data may be retrieved: (1.) Active, online data, such as information on hard drives; (2.) Near-line data, such as data stored on optical discs and retrieved using a robotic device; (3.) Offline storage/archives, such as removable optical disk or magnetic tape media, which can be labeled and stored in a shelf or rack; (4.) Backup tapes; and, (5.) Erased, fragmented or damaged data. Of these, the first three categories are typically identified as accessible, and the latter two as inaccessible. The cost of retrieving these data, generally speaking, increases as the speed of retrieving the data declines.

1. Active, Online Data

These data are the files used in the very active stages of an electronic record's life: when it is being created or received and processed, as well as when the access frequency is high and the required speed of access is very fast, *i.e.*, milliseconds. Records that fall within this category would include email, current word processing and spreadsheet documents, and so forth.

Email deserves special consideration in this context, because there is nothing like it in the "paper" world. Several characteristics of email make it problematic. In part, email is problematic because there is just so much of it. Communications that once took place over the phone or at the water cooler are now reduced to light, breezy, often-misspelled (and therefore hard to search) messages. Another problem is that email systems are seldom designed for file management and retrieval, resulting in relevant email messages being saved along with irrelevant and often very private personal email messages. These factors combine to make computer-based word-searching difficult, and screening for relevance and privilege costly and time-consuming. But these characteristics of email also make it a most attractive target for discovery.

Because email messages are so often written in an unguarded, candid, and honest fashion, it is

often perceived to offer the mother lode of proof. Certainly, few written documents (outside of private diaries) provide as clean a view of a decision maker's thought processes. There is, however, an often overlooked "hidden" aspect to the day-to-day electronic records that deserves scrutiny, the "metadata" embedded in electronic versions of documents.

For example, any given Microsoft Office file may contain the following information stored as metadata: the user's name, initials, and company or organization name; the name of the computer on which the file was created; the name of the network server or hard disk where the user saved the file; other file properties and summary information including creation, access, and modification dates and times; the names of previous file authors; document or spreadsheet versions; document or spreadsheet revisions; template information; hidden text; and comments.³ These metadata are buried within the electronic record of the document. The embedded metadata can pin down the entire process of the document's creation and reveal much more than the paper version of a letter or memo – sometimes just the last in a long line of behind the scenes discussions of how to spin the situation. Little else, including witness memories or deposition questioning, can recreate as well the sequence of events of when and how the document was created.

2. Near-line Data

Near-line data typically consists of a robotic storage device (robotic library) that houses removable media, uses robotic arms to access the media, and uses multiple read/write devices to store and retrieve records. Access speeds can range from as fast as milliseconds if the media is already in a read device, up to 10-30 seconds for optical disk technology, and between 20-120 seconds for sequentially searched media, such as magnetic tape.

3. Offline Storage/Archives

This is removable optical disk or magnetic tape media, which can be labeled and stored in a shelf or rack. Offline 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 offline media involves manual intervention and is much slower than online or near-line storage. Access speed may be minutes, hours, or even days, depending on the access-effectiveness of the storage facility.

In a perfect world, these offline, archival electronic files should be organized for identification and retrieval of individual documents or series of records and, as employers adopt new computer systems, the data from older systems should be transferred to new media. In reality, though, such electronic records management processes are primitive or non-existent in many organizations. Generally, offline data lacks the coordinated control of

a computer hard drive, and is, in the lingo, JBOD ("Just a Bunch Of Disks").

As part of the initial meet and confer process, counsel for both sides should make a realistic assessment of the extent to which these files will be subject to discovery and how much it will cost to make these files searchable.

4. Backup Tapes

Backup tapes rely on a device, like a tape recorder, that reads data from and writes data onto a tape. Tape drives have data capacities of anywhere from a few hundred kilobytes to several gigabytes. Most businesses periodically back up their data onto tapes for disaster recovery purposes. Often these tapes are kept for months on a rotating basis. Data and documents that have been edited, deleted, or written over in the normal course of business may be recovered from these tapes or disks.

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. As a result, the 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. 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 governing data compression. Often, special programs are required to retrieve the information.

Backup tapes are clearly discoverable, but at least one court has ruled that the burden of retrieving the information from tape backups is enough to require cost-shifting to the requesting party. *Zubulake v. UBS Warburg LLC (Zubulake III)*, 216 F.R.D. 280 (S.D.N.Y. 2003). Counsel should be prepared to demonstrate that this discovery is necessary and germane to the case. Before the Rule 26(f) pretrial conference, the employee's counsel should determine whether discovery of backup data is expected, and weigh the value of this discovery against its likely high cost.

5. Erased, Fragmented, or Damaged Data

When a file is first created and saved, it is laid down on the disk storage media in contiguous clusters. As files are erased, their clusters are made available again as free space. Newly created files that are too large to fit in contiguous spaces are 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.

An examination of erased, fragmented, or damaged data requires an inspection of the data storage medium (usually a hard drive) itself. Typically, this is not only extremely expensive but exceptionally disruptive to the party responding to the discovery request. Over the past several years, federal courts

have evolved a protocol for conducting this type of inspection.⁴ The procedure typically employs the following elements:

- The parties agree on a neutral, third-party expert who will actually carry out the inspection as an officer of the court.
- The parties, with the assistance of either their own experts or with the assistance of the neutral expert, agree on the scope of the inspection, including target computers or servers; target individuals, departments, or data collections; date ranges; search terms; or other scope-defining criteria. They also agree upon the form of eventual production.
- The expert creates a copy of the computer data or of the computer media using accepted computer forensic procedures that preserve the integrity of the original evidence. Usually, this involves taking the subject computer off-line and making a physical sector-by-sector copy of the hard drive.
- Unless the examination requires a search for “ghost” images on the inspected hard drive,⁵ the expert executes the search on the “mirror image” and identifies relevant data according to the agreed-upon specifications. If the examination requires in-depth forensic study of the original, then the “mirror image” is returned to service in place of the original.
- The expert turns over the responsive data to the respondent’s counsel.
- Respondent’s counsel reviews the responsive data for relevance and privilege.
- Respondent’s counsel produces relevant, non-privileged data to the requesting party in the form agreed upon by the parties.

It should be noted that the enormous expense involved in using forensic data recovery experts, as well as the inconvenience caused by their investigations, have led at least one court to refuse to order a “neutral” expert unless the party making the request can show that the opposing party has tried to mislead the court or has made some substantively inaccurate statement regarding the completeness of its production.⁶

Save The Forest: Electronic records should be produced in electronic form

Many electronic records, such as relational databases, email stores, and spreadsheets, are meaningless in printed form. The recipient is forced to reenter the data or spend long hours performing manual analysis. Moreover, printing a document deprives the recipient of its metadata. In this regard, producing printouts of computer data is so unnecessary and evasive that it might be considered an abusive tactic. To avoid unnecessary costs and delay, courts have ordered production in electronic form even if it duplicates prior paper production or involves the creation of tapes or disks that did not hitherto exist.

Of course, even if the parties agree to exchange

computer data in electronic form, there is still room for argument over which electronic format the data should take. As with most of the other issues raised in this article, the best way to resolve these problems is by consulting with an expert (once the choices of format are known) and by meeting and conferring with opposing counsel early in the process to establish common procedures and formats for the production of electronic information at the outset of discovery. Under one of the proposed amendments to Rule 26(f), counsel in federal cases are required to make the determinations as part of their pretrial conference on a plan of discovery.

Out of Order, Chaos: Inadvertent, negligent, reckless, and intentional data spoliation **Inadvertent Data Loss**

As discussed above, computer operating systems, and the Microsoft Windows operating system in particular, do not actually erase the file data from the hard drive at the time a file is deleted. The delete command causes Windows to mark the file space as being available by changing one character in the file table.⁷ With that change, Windows itself is free to overwrite the file data.⁸ Over time, the chance that an unallocated file space will be overwritten with new data is substantial. Entering data, loading software, performing routine system maintenance or simply booting a computer can destroy files and metadata that are stored on the hard drive (e.g., key facts about the data, such as its creation, last access, or last modified dates).⁹

Thus, an employer who negligently, or merely ignorantly, continues to use a computer after it has become aware of an employee’s claim can be guilty of destroying evidence. Imposition of sanctions for spoliation does not require a showing that the evidence was destroyed in bad faith.¹⁰ If, however, bad faith is present, a court may impose the ultimate sanction of striking a party’s pleadings.¹¹ With this in mind, the Advisory Committee on Civil Rules has proposed alternative amendments to Federal Rule of Civil Procedure 37. The first, which appears to be the favored version, provides a safe harbor from spoliation sanctions for a party that takes reasonable steps to preserve electronically stored information but loses the information as a result of the “routine operation of the party’s electronic information system.” A second version, offered by the Advisory Committee to inspire debate on the matter, provides a much broader safe harbor provision, forbidding sanctions unless the offending party acted recklessly or intentionally in allowing the data to be lost.

At the moment, therefore, an employer may be liable for inadvertent spoliation of electronic records. In the near future, the employer may have a safe harbor, depending upon which, if either, of the proposed rule changes takes effect.

Intentional Spoliation

An employer who stands by idly after being put

on notice of a legal claim under federal law and fails to implement does so at considerable risk. This includes the implementation of email retention policies of very short duration as a passive way to effect the destruction of relevant electronic data and documents. An improper, unreasonable or unenforceable document retention policy may be viewed in the same light as no electronic retention policy at all.¹²

Within the context of a case involving unlawful employment practices, the employer's duty to preserve electronic records begins when the employer is first on notice that the evidence is potentially relevant or reasonably likely to be requested during discovery.¹³

In similar fashion, Virginia courts have held that a litigant has a duty to preserve evidence that "a reasonable person in the defendant's position should have foreseen . . . was material to a potential civil action."¹⁴

Under either state or federal law, the general rule governing the duty to preserve evidence is that a party is under a duty to preserve what it knows, or reasonably should know, is relevant to the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery, and/or is the subject of a pending discovery request.¹⁵

A Case Study of Electronic Discovery in the Employment Law Context: The *Zubulake* opinions

No meaningful discussion of electronic discovery in an employment case can take place without consideration of the groundbreaking case of *Zubulake v. UBS Warburg*. In that case, which was based of a claim of gender discrimination, Judge Shira Scheindlin of the Southern District of New York issued a series of opinions ruling definitively on a variety of electronic discovery issues. In *Zubulake I*, 217 F.R.D. 309 (S.D.N.Y. 2003) and *III*, 216 F.R.D. 280 (S.D.N.Y. 2003), the plaintiff issued a request for production seeking "[a]ll documents concerning any communication by or between UBS employees concerning the plaintiff," with the term "document" defined as including, "without limitation, electronic or computerized data compilations." UBS produced 350 pages of documents, inclusive of approximately 100 pages of email. *Zubulake* was aware of the existence of additional responsive email, as she herself had produced roughly 450 pages of email correspondence. The defendant claimed undue burden and expense, and urged the court to shift the cost of production to the plaintiff. The Court stated that cost-shifting should only be considered when electronic data is relatively inaccessible (as it was in this case), and considered the eight-factor cost-shifting test set out in *Rowe Entm't, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421 (S.D.N.Y. 2002).

The Court determined that the application of the

Rowe factors might in fact result in disproportionate cost shifting away from large defendants, and modified the test so that it consisted, instead, of the following seven factors: 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 information.

The Court ordered UBS to produce, at its own expense, all responsive email existing on its optical disks, active servers, and five backup tapes selected by the plaintiff, determining that only after the backup tapes were reviewed and the defendant's costs quantified would the court conduct the aforementioned cost-shifting analysis.

In *Zubulake IV*, 220 F.R.D. 212 (S.D.N.Y. 2003), during the review of backup tapes previously ordered, the plaintiff discovered that certain backup tapes were missing and certain responsive emails had been deleted. *Zubulake* moved for sanctions against UBS for its failure to preserve the responsive evidence. The Court found that the defendant had a duty to preserve the missing evidence, as it should have known that the emails might be relevant to future litigation (UBS had clear reason to suspect that it might be party to a suit by *Zubulake* well in advance of her filing suit). The Court further found that UBS failed to comply with its own document retention policy, which, had it been followed, would have preserved the missing tapes and emails. However, the Court stated that despite defendant's culpability for the destruction of the electronic evidence, *Zubulake* could not prove that said evidence would have supported her claims. Thus, the Court held that an adverse inference instruction to the jury was not appropriate; nevertheless, the Court awarded the plaintiff costs for re-deposing witnesses for the purpose of gathering evidence regarding the destruction of electronic materials and the existence of any newly-discovered email.

In 2004, the Court issued *Zubulake V*, 2004 U.S. Dist. LEXIS 13574 (S.D.N.Y. July 20, 2004). *Zubulake V* addressed a motion by the plaintiff for sanctions against UBS in the form of an adverse inference jury instruction for the defendant's continued failure to produce relevant email and the prejudice caused to the plaintiff by defendant's delay in producing certain recovered email that was ultimately produced by UBS. The Court found that UBS had willfully deleted relevant email in contravention of court orders, and granted the motion for sanctions, also ordering the defendant to pay costs. The Court further noted that counsel was responsible for coordinating the client's discovery evidence,

and therefore partly to blame for the document destruction due to its failure to locate, preserve, and timely produce the relevant information. The Court stated that “[c]ounsel must take affirmative steps to monitor compliance so that all sources of discoverable information are identified and searched,” and that counsel must guarantee that potentially relevant information is preserved by placing a “litigation hold” on potentially relevant documents, communicating to employees the import of preservation of the documents, and ensure that all relevant archival media is identified, segregated, and stored in a safe location.

In March, 2005, the most recent *Zubulake* opinion (“*Zubulake VI*”), 2005 U.S. Dist. LEXIS 4085 (S.D.N.Y. 2005), was issued, revisiting, among other matters, a number of the electronic discovery issues that were addressed in prior decisions in the case. The Court granted a motion by UBS to preclude the introduction of evidence regarding the court’s previous decisions in the case, including the imposition of sanctions on the defendant, agreeing that the previous five decisions were irrelevant to the plaintiff’s claims and would unfairly prejudice UBS. The defendant also moved to exclude any correspondence between counsel on discovery matters, arguing that such correspondence was irrelevant to the plaintiff’s claims and to the adverse inference jury instruction. The Court observed that the adverse inference instruction stated, in pertinent part, “You may also consider whether you are satisfied that UBS’ failure to produce this information was reasonable.” In light of the instruction, the Court held that the plaintiff would be entitled to introduce correspondence between counsel on discovery matters if the defendant opened the door by introducing evidence as to whether the failure to produce was reasonable. If UBS declined to offer proof that the failure to produce certain email (or late production of other email) was reasonable, the plaintiff would not be allowed to introduce any of the correspondence between counsel in her case in chief. UBS further sought to preclude the introduction of evidence concerning its failure to preserve the aforementioned backup tapes. The Court noted that the destruction of the tapes might be relevant to the defendant’s justification for failing to produce certain emails; however, the Court concluded that, again, *Zubulake* would be permitted to introduce evidence of backup tape destruction “if, and only if,” UBS opened the door to such evidence. Finally, the Court granted the defendant’s motion to preclude testimony from its counsel at trial, since the plaintiff had indicated that she intended to elicit testimony from UBS’ counsel regarding the preservation of emails and backup tapes. The Court reasoned that “the risk that privileged communications could be probed during trial is arguably too great to permit plaintiff to call opposing counsel to testify,” and that plaintiff did not appear to have any

legitimate need for calling opposing counsel in light of the extensive discovery on the issue electronic preservation and retention.

In April 2005, U.S. District Judge Scheindlin instructed the jury to assume that emails UBS discarded after *Zubulake* filed her EEOC complaint would have hurt the bank’s case. Following a trial in which the compensatory and punitive damages portions were bifurcated, the jury awarded \$9.1 million in compensatory damages and \$20.2 million in punitive damages in favor of *Zubulake* and against UBS. It is fair to surmise, under these circumstances, that UBS’s destruction of evidence played a role in the calculation of the punitive damages award.

Conclusion

Electronic discovery has overtaken traditional discovery in large cases and, before much longer, will overtake traditional discovery in almost every case, as society trends away from paper documents and more and more information is created and stored digitally. The Federal Rules of Civil Procedure are being amended for the purpose, by and large, of placing a greater burden on counsel to anticipate and proactively resolve discovery disputes during the early meet-and-confer stages of litigation. In this regard, the attorney who has the better understanding of how electronic records work will have the advantage in shaping the course of the lawsuit.

Endnotes

1. *Applied Telematics, Inc. v. Sprint Communications, Inc.*, 1996 U.S. Dist. LEXIS 14053 (E.D. Pa. Sept. 17, 1996); *Lewy v. Remington Arms Co.*, 836 F.2d 1104 (8th Cir. 1988); *Thompson v. General Nutrition Co.*, 593 F. Supp. 1443 (C.D. Cal. 1984).
2. By the same token, the employee plaintiff should be preserving his or her own evidence. Questions to ask a client to determine what to preserve might include: Do you have a computer in your office? Do you have a computer at home? Do you have access to the internet? Do you use email? Do you use voice or phone mail? Do you use some form of electronic calendar or address book or a PDA? An affirmative answer to any of these questions should lead counsel to strongly consider having a forensically sound copy made of the employee’s electronic data as quickly as possible. Another area of concern for employee’s counsel is whether and to what extent the employee has engaged in “self-help” prior to seeking a lawyer. For more on this, see the accompanying article on the Virginia Computer Crimes Act.
3. See Microsoft, “How to minimize metadata in Office documents,” at <http://support.microsoft.com/kb/q223790> (last visited June 20, 2005). In this article, Microsoft offers this advice: “Whenever you create, open, or save a document in any of the programs listed

at the beginning of this article, the document may contain information that you may not want to share with others if you distribute the document electronically.” The programs to which this article applies include Microsoft Excel 2002 Standard Edition; Microsoft PowerPoint 2002 Standard Edition; Microsoft Word 2002 Standard Edition; Microsoft Excel 2000 Standard Edition; Microsoft PowerPoint 2000 Standard Edition; Microsoft Word 2000 Standard Edition; Microsoft Excel 97 Standard Edition; Microsoft PowerPoint 97 Standard Edition; and Microsoft Word 97 Standard Edition. *Id.*

4. See *Playboy Enterprises, Inc. v. Welles*, 60 F. Supp. 2d 1050 (S.D. Cal. 1999); *Northwest Airlines, Inc. v. Local 2000, Int’l Bhd. of Teamsters*, 2000 U.S. Dist. LEXIS 22638 (D. Minn., 2000); *Simon Property Group, L.P. v. MySimon, Inc.* 33. 167 F.R.D. 90 (D. Colo. 1996).
5. One species of forensic data recovery relies on the fact that computer discs have tracking errors, i.e., the disc does not spin in a perfect circle and the part that reads and writes information to the disc doesn’t always hit the disc in the same place. As a result of this tracking error, new data do not overwrite the old data completely, and a data recovery specialist may discover disc sectors that were not totally erased.
6. See *Williams v. Mass. Mut. Life Ins. Co.*, 226 F.R.D. 144, 146 (D. Mass., 2005).
7. See Canter, Sheryl, “All Is Not Lost,” PC Magazine, October 1, 2003, at <http://www.pcmag.com/article2/0,1759,1265112,00.asp> (last visited June 20, 2005); Microsoft, How to Locate and Correct Disk Space Problems on NTFS Volumes in Windows XP, at <http://support.microsoft.com/?scid=kb;en-us;315688&spid=1173&sid=1230> (last visited February 19, 2005) Microsoft briefly describes the process of file allocation as follows: “After you create and format an NTFS volume, NTFS metafiles are created. One of these metafiles is called the “Master File Table” (MFT). This file is very small when it is created (approximately 16 KB), but it grows as files and folders are created on the volume. When a file is created, it is entered into the MFT as a file record segment, which is always 1024 bytes (1 KB) in size. As files are added to the volume, the MFT grows as required. However, when you delete files, the associated file record segments are marked as free to be reused, but the total file record segments and associated MFT allocation remains the same.”
8. Windows may do this by allocating the address to new “permanent” files or by overwriting the address with “swap” files, which Windows uses to temporarily store data that are too large to fit in the computer’s random access memory (RAM) or which are being sent to an output device like a printer. See, Microsoft, How To Move the Spool Folder in Windows XP, at <http://support.microsoft.com/default.aspx?scid=kb;en-us;308666&sd=tech> (last visited June 20, 2005); Microsoft, How to configure paging files for optimization and recovery in Windows XP, at <http://support.microsoft.com/?kbid=314482> (last visited June 20, 2005).
9. See “Examining the Data: A beginners guide to com-

puter-based evidence,” by Kristin M. Nimsger, Esq. and Michele C.S. Lange, *Security Products*, May 2002, p.16, republished by permission at www.krollontrack.com/Publications/securityproducts.pdf (last visited June 20, 2005).

10. *Trigon Ins. Co. v. United States*, 204 F.R.D. 277, 287 (E.D. Va. 2001).
11. See *Gentry v. Toyota Motor Corporation*, 252 Va. 30, 34, 471 S.E.2d 485, 488 (1996) (spoliation of material evidence is a ground for dismissal where it results from bad faith of a party); *Wade v. Fleetwood Homes of N.C., Inc.*, 2001 Va. Cir. LEXIS 535 (Cir. Ct. Nelson County, 2001).
12. See *In re Prudential Ins. Co. of America Sales Practices Litigation*, 169 F.R.D. 598 (D.N.J. 1997) (after repeated violations of a freeze order, court fined Prudential \$1 million, ordered Prudential to pay plaintiffs’ attorneys’ fees and costs, ordered that Prudential mail each employee a copy of court’s order prohibiting the destruction of documents, and other sanctions).
13. *Applied Telematics, Inc. v. Sprint Communications, Inc.*, 1996 U.S. Dist. LEXIS 14053 (E.D. Pa. Sept. 17, 1996); *Lewy v. Remington Arms Co.*, 836 F. 2d 1104 (8th Cir. 1988); *Thompson v. General Nutrition Co.*, 593 F. Supp. 1443 (C.D. Cal. 1984).
14. *Wolfe v. Virginia Birth-Related Neurological Injury Compensation Program*, 40 Va. App. at 581, 580 S.E.2d at 475 (citation omitted).
15. *Turner v. Hudson Transit Lines, Inc.*, 142 F.R.D 68, 72 (S.D.N.Y. 1991).



Harris D. Butler, III is a founding partner of Butler Williams & Skilling P.C., in Richmond and heads the firm’s employment team. His practice areas include employment discrimination, sexual harassment, wrongful discharge and civil rights. He is a graduate of Texas A&M University and the University of Houston School of Law. He is also active in numerous bar associations.



Rebecca Royals is an October 2005 admittee to the Virginia State Bar. She is a graduate of Louisiana State University and recently received her J.D. from the University of Richmond’s T.C. Williams School of Law. While a law student, Ms. Royals clerked at Butler Williams & Skilling, P.C., in the employment law and insurance defense sections.



Blackwell N. Shelley, Jr., works extensively in the law of discrimination and wrongful termination and in other areas such as covenants not to compete, protection of trade secrets and creditors’ rights. A graduate of the University of Virginia and the Washington & Lee University School of Law, he practices in Richmond with Butler Williams & Skilling P.C.



Tim Schulte, of Butler Williams & Skilling P.C. in Richmond, practices in the employment law, civil rights and general civil litigation areas. Mr. Schulte attended the Georg-August Universitat School of Law in Germany, received his LL.M. from the Marshall-Wythe School of Law and his J.D. from the University of Richmond’s T.C. Williams School of Law.

The flip side for employees: Virginia Computer Crimes Act

Increasingly, and particularly in cases involving employees who telecommute or who have access to an employer's computer system, an employee's use of the employer's computer system both pre- and post-termination will likely be subject to intensified scrutiny once the employer becomes aware of the employee's claim. Some employees may engage in self-help prior to seeking a lawyer's assistance and investigate the employer's computer network for evidence of employer wrongdoing. If this is the case, counsel for the employee should look closely at his or her client's behavior, prior to proceeding, to determine whether the employee is exposed to criminal or civil liability.

The preservation of potentially relevant electronic evidence is not the only issue confronting the legal field as data are increasingly stored in electronic form; more and more confidential data are among that retained electronically, and as a result, it is relatively simple to access and download or otherwise obtain such confidential information without consent or permission. Virginia Code §§18.2-152.2-152.15 creates criminal penalties and civil causes of action for Computer Fraud (§18.2-152.3); Computer Trespass (§18.2-152.4); Computer Invasion of Privacy (§18.2-152.5); Theft of Computer Services (§18.2-152.6); and Personal Trespass by Computer (§18.2-152.7). Civil remedies are found at Va. Code §18.2-152.12, and include damages (including but not limited to lost profits) and costs of suit. The statute makes clear that the use of this action does not limit the use of other civil remedies – for instance, violation of the Act would clearly constitute an “improper method” sufficient to support a claim for tortious interference with an at-will contract.

The Act remains relatively untested at this time, with scant case law to define the Act's parameters. Of the civil cases applying the Act, several offer more salient decisions. In *Perk v. Vector Resources Group, Ltd.*, 253 Va. 310 (1997), the Virginia Supreme Court held that an attorney hired by a hospital for collections work stated a claim under the Act sufficient to overcome demurrer by alleging that after the termination of his relationship with the hospital, another firm misappropriated a computer program that he had designed to perform his collection responsibilities. The Fairfax Circuit Court provided an expansive interpretation of the Act in *S.R. v. Inova Healthcare Services*, 49 Va. Cir. 119 (Fairfax Co. 1999), when it overruled a demurrer to a civil claim by a patient alleging computer invasion of privacy. In that case, the employees of one hospital allowed nurses from another hospital to access computer records pertaining to the patient's medical care. In contrast, however, the Court's ruling in *McGladrey & Pullen, LLP v. Shrader*, 62 Va. Cir. 401 (Rockingham Co. 2003), constricted the power of the Act by sustaining a demurrer to punitive damages under the Act because the Act contains no specific provision for punitive damages. As of the date of this writing, no other court has ruled on this issue, leaving this tiger, at least for the present, short a few teeth.

Computer Trespass is a Class 3 misdemeanor (and a Class 1 misdemeanor for reckless disregard resulting in property damage of up to \$2,500; a Class 6 felony for malicious property damage of \$2,500 or more). It is also the basis for a civil action pursuant to §18.2-152.12. Included in the definition of Computer Trespass are: temporarily or permanently removing, halting, or otherwise

disabling any computer data, computer programs, or computer software from a computer or computer network; altering or erasing any computer data, computer programs, or computer software; making or causing to be made an unauthorized copy, in any form, including but not limited to, any printed or electronic form of computer data, computer programs, or computer software residing in, communicated by, or produced by a computer or computer network. In *CigarCafe, L.C. v. America Online, Inc.*, the Alexandria Circuit Court noted that under the Computer Trespass component of the Act, any person that uses a computer or network beyond his or her authority may be liable for computer trespass. However, where the owner of a computer network deprives a customer of benefits of or access to the network, this may constitute a breach of contract, but is not a computer trespass. 50 Va. Cir. 146 (City of Alexandria 1999).

The Virginia Computer Crimes Act defines “computer” as “an electronic, magnetic, optical, hydraulic or organic device or group of devices which, pursuant to a computer program, to human instruction, or to permanent instructions contained in the device or group of devices, can automatically perform computer operations with or on computer data and can communicate the results to another computer or to a person.” Conceivably, this definition classifies as a computer everything from a PC to a cell phone to a late-model car. The definition of “computer data,” likewise, is very broad, encompassing “any representation of information, knowledge, facts, concepts, or instructions which is being prepared or has been prepared and is intended to be processed, is being processed, or has been processed in a computer or computer network. ‘Computer data’ may be in any form, whether readable only by a computer or only by a human or by either, including, but not limited to, computer printouts, magnetic storage media, punched cards, or stored internally in the memory of the computer.” The Act goes on to define the terms “computer network,” “electronic mail service provider” and “person.” Under the definitions provided in the Act, printouts, computers, personal digital assistants (PDAs) and even data stored on cellular phones are protected. As the field of e-discovery continues to be shaped by legislation and court rulings, the definitions provided in the Virginia Computer Crimes Act may well provide guidance to Virginia courts seeking to establish electronic discovery precedent.

Rebecca Royals