

LITIGATION REVIEW

UP-TO-DATE ANALYSIS FOR CLIENTS AND FRIENDS OF THE FIRM

The Changing World Of Electronic Discovery

STEVEN J. CISZEWSKI

Without question, developments in wireless and electronic communications technology have made it easier to keep in touch with the office at any time of day and from any place in the world. But this technology also has given rise to many new issues for management, in-house attorneys and outside counsel when a legal dispute occurs. When faced with the threat of litigation, the days of simply going to the filing cabinet to collect the relevant paper documents and files are over. The legal team must now quickly identify, preserve and work with the electronic data stored on office computers, home computers, laptop computers, e-mail servers, other network servers, system back-up files or tapes, PDAs and more.

The purpose of this article is to present a basic overview of the types of electronic data that are frequently sought in litigation and that should be identified and preserved once a risk of litigation arises. We will then discuss some of the consequences (many quite harsh) for the litigant who fails to take immediate steps to identify and preserve this data. Finally, we will provide some basic guidelines for electronic data management that should be considered at all times and certainly implemented when the risk of litigation materializes.

One final note before proceeding to these topics. There are many complications and issues relative to electronic data that cannot possibly be addressed in this one article. Whether taking preventative measures now – or when implementing a data retention plan when the litigation risk ripens – the first step should be to involve the entire legal team, including outside counsel, to quickly establish a protocol for the preservation of data. The exact steps and precautions must be analyzed on a case-by-case basis,

and nothing in this article or any of the cases cited herein provides a fail-safe means of electronic data preservation in all cases.

The Broad Scope Of Electronic Discovery

Courts have left no doubt that electronic data is within the scope of discovery allowed in litigation. *Thompson v. U.S. Dept. of Housing and Urban Dev.*, 219 F.R.D. 93, 96 (D. Md. 2003) (collecting cases).

Indeed, by the end of the year, an expansive amendment to the Federal Rules of Civil Procedure is expected to be in place. These proposed new rules make explicit the key role that the discovery of electronic data plays in current lawsuits. Specifically, the proposed rules describe the scope of discovery as including all “documents or electronically stored information – including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained . . .” (Proposed Fed. R. Civ. P. 34(a).) The comments to this proposed rule further clarify “that discovery of electronically stored information stands on equal footing with discovery of paper documents” and that the proposed rule “is intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and developments.” (Comments to Proposed Fed. R. Civ. P. 34(a).)

Proposed Rule 34 also sets forth certain guidelines about how the electronic discovery process should work. For example, it permits the requesting party to “specify the form or forms in which electronically stored information is produced.” (Proposed Fed. R. Civ. P. 34(b).) The comments explain that, given current technology, electronic data may be stored in many different manners – (*i.e.*, word

processing documents, e-mails, electronic spreadsheets, and image and sound files). Depending on the circumstances, the requesting party may want some types of data produced electronically (*i.e.*, large spreadsheets) and other types of data produced in paper form (*i.e.*, e-mails). The responding party does, however, have the ability to object to a designation by the requesting party and/or make a counter-designation regarding the format of production if the requesting party does not do so. The comments encourage the parties to discuss the format of the production of electronic data at an early stage to allow for the most efficient and cost-effective exchange of information.

Finally, the proposed rule requires that the responding party produce electronic data in its normal format or in a format that is “reasonably usable.” The comments caution that in some circumstances, this may require the producing party to “provide some reasonable amount of technical support, information on application software, or other reasonable assistance to enable the requesting party to use the information.” (Comments to Proposed Fed. R. Civ. P. 34(b).)

Some individual states also have adopted court rules explicitly stating that electronic data falls within the scope of discovery in litigation. In Illinois, for example, Supreme Court Rule 201(b)(1) explicitly includes within the scope of discovery “all retrievable information in computer storage.” Similarly, the California Code of Civil Procedure explicitly includes electronic mail within the scope of discovery. (Cal. Civ. Proc. Code §2016.020, incorporating Cal. Evid. Code §250.)

Sources Of Electronic Data

Given that electronic data is clearly within the scope of discovery, it is important for the legal team to identify the many potential sources that will need to be searched when the threat of litigation arises. Of course, the actual sources of electronic data will vary on a case-by-case basis. However, there are some typical areas that should be searched in all

cases – and the search expanded, if necessary, depending on the details of the specific case.

Courts have given the following examples of electronic data that is subject to discovery: voice mail, e-mail, deleted e-mail, data files, program files, back-up files, archival tapes, temporary files, system history files, web site information in textual, graphical or audio format, web site files, cache files and “cookies.” *E.g.*, *Thompson*, 219 F.R.D. at 96. As noted, the key in any individual case is to quickly consult with the legal and information technology team in order to identify all potential sources of electronic data in your specific case.

One potential location of electronic data – deleted files – is a common source of confusion. When a user deletes an electronic file (for example, by deleting a file from the hard drive), that data is not necessarily immediately erased. *Id.* at 97. Rather, that data is simply designated as not in use so that the computer knows that it may be overwritten in the future. *Id.* Thus, courts have held that deleted files which have not been overwritten are within the permissible scope of discovery. *Id.* See also *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 317 (S.D.N.Y. 2003). This level of detail should be enough to demonstrate that it is very important to immediately consult with the information technology staff to make sure these more obscure sources of data are identified and preserved.

Duty To Preserve Electronic Data

We know that there is a vast universe of electronic data and that it is discoverable in litigation. The next question is what duty do litigants (and potential litigants) have to preserve their electronic data. The timing and scope of this duty require special attention because many data storage and computer systems automatically purge old files and/or re-write over them. Indeed, the normal daily shut-down operations of a computer may delete potential sources of electronic data.

Probably the most well-known and oft-cited case in the realm of electronic discovery is *Zubulake* – a gender discrimination and retaliatory discharge case brought by Zubulake against her former employer. In that case, the court issued a series of lengthy written opinions addressing the former employer’s duty to preserve e-mail archives and back-up tapes and the consequences for its failure to do so.

The *Zubulake* court held that the duty to preserve electronic data “arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation.” *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003). Under this standard, it is clear that the duty arises no later than the date that litigation is filed or a claim asserted. Under the facts in *Zubulake*, for example, the court found that the duty of preservation necessary arose as soon as Zubulake filed her EEOC claim (in August 2001). *Id.*

However, *Zubulake* went further to hold that the duty of preservation may arise even before a formal lawsuit or charge is filed. In that case, there was evidence that Zubulake’s former work colleagues feared that she would sue as early as April 2001 (four months before Zubulake’s EEOC claim was filed). *Id.* at 216-17. Thus, *Zubulake* held that the relevant people anticipated litigation in April 2001 and that the duty of preservation, therefore, was triggered at that time. *Id.* at 217.

Once the duty of preservation is triggered, the next issue is what exactly needs to be preserved. Courts generally reject the idea that all electronic data need be preserved, because to require that would cripple most corporations. *Id.* *Zubulake*, for example, held that the duty of preservation extends to all “unique, relevant evidence that might be useful to an adversary.” *Id.* With respect to this requirement, *Zubulake* holds that at least one copy of all relevant electronic data must be retained. *Id.* However, according to *Zubulake*, the retaining party has the option to keep this data in the format (*i.e.*, electronic file, paper or other format) that is most convenient for it. *Id.* at 218. Thus, the party in

possession of electronic data is well advised to retain at least one copy of all relevant electronic data in the format that is most convenient, least expensive and causes the least long-term impact upon on-going operations.

Zubulake further holds that the duty of preservation extends to all e-mails sent by or to “those employees likely to have relevant information – the ‘key players’ in the case.” *Id.* This includes all e-mails to or from such “key players” that may bear on the subject matter of the dispute. The duty also includes data from their PDA, laptop computer, and any electronic files that they created or worked on (*i.e.*, their Microsoft Word, Excel and other similar files). *Id.*

Zubulake summarized the scope of the duty to preserve as follows: “Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a ‘litigation hold’ to ensure the preservation of relevant documents.” *Id.*

Consequences For Failing To Preserve Electronic Data

The consequences for breaching the duty of preservation can be quite severe. Courts have the authority to issue a wide variety of sanctions for discovery abuses, including a party’s failure to satisfy its duty to preserve and produce electronic data. For example, the Federal Rules of Civil Procedure explicitly authorize courts to impose sanctions for discovery abuses and/or non-compliance with court orders including, without limitation: (a) taking certain facts as true; (b) prohibiting the non-compliant from introducing evidence on certain topics; (c) striking pleadings; and (d) entering default judgment. (Fed. R. Civ. P. 37.) Likewise, the Illinois Supreme Court Rules explicitly authorize similar sanctions for certain discovery abuses and/or non-compliance with court orders. (Illinois Supreme Court Rule 219.)

Applying these and similar rules – as well as their own inherent authority to govern the cases before them – courts

have taken a variety of approaches to the destruction of electronic data. In this context, the following three potential sanctions are discussed quite often: (a) default judgment/dismissal; (b) an adverse inference; and (c) restricting the use of electronic data as evidence. Although a full discussion of how and when these sanctions may be applied is beyond the scope of this article, the following discussion will describe factors that may govern the severity of the sanction considered for the mishandling of electronic data.

1. DISMISSAL/DEFAULT JUDGMENT

The most severe sanction—dismissal—was recommended in *Kucala Enter., Ltd. v. Auto Wax Co., Inc.*, No. 02 C 1403, 2003 WL 21230605 (N.D. Ill., May 27, 2003); *adopted as modified* at 2003 WL 22433095 (N.D. Ill., Oct. 27, 2003). In *Kucala*, the plaintiff installed and ran a program called Evidence Eliminator on his computer. *Id.* at 1. Evidence Eliminator was advertised to totally scrub the hard drive by permanently deleting all data, including the residual data that is embedded in the drive even after the user deletes those files. *Id.* at 2. As a sanction for using Evidence Eliminator, the Court recommended the dismissal of the claims related to the evidence destroyed and the award of certain attorneys' fees. *Id.* at 8.

The *Kucala* court reached two important conclusions that seem to be applicable even outside the fact setting in that case. First, the court noted that dismissal is an appropriate sanction where the litigant's conduct is objectively unreasonable or in bad faith. Thus, an argument that the litigant subjectively did not know he was permanently deleting files or did not know the files were relevant to the litigation may not insulate that litigant against the sanction of dismissal. It is an objective – not subjective – analysis.

Second, the court did not require there to be a showing of what files were actually deleted and/or that those files contained relevant information. It was enough that a

large volume of files was deleted under those extreme circumstances. *Id.* at 6.

A case like *Kucala* demonstrates that the use of scrubbing software after the preservation duty has arisen will be viewed the same way as a litigant using a paper shredder to destroy hard copy documents. It is subject to the most severe of sanctions and should not be attempted.

2. ADVERSE INFERENCE

A less severe, but still crippling sanction for the destruction of electronic data is an adverse inference or jury instruction. Under this sanction, the court may instruct the jury that, if it finds a party had electronic data within its control and that this data was destroyed, then the jury can infer from those facts that the electronic data was damaging to that party's case. *E.g., Mosaid Tech. Inc. v. Samsung Elec. Co., Ltd.*, 348 F. Supp. 2d 332, 334 (D.N.J. 2004).

The predominant purpose of an adverse inference is to “level the playing field after a party has destroyed or withheld relevant evidence.” *Id.* at 338. Regardless of its purpose, the introduction of such an instruction at trial could very well be the deciding factor for the jury, regardless of all other facts. Accordingly, while identified as a lesser sanction, it still may have an outcome-determinative effect. Because this is a frequently considered sanction, we provide three detailed case studies which provide examples of how and when this sanction might be applied.

A. Case Study: *Zubulake*

In *Zubulake*, certain e-mail back-up tapes were missing and/or were destroyed. *Zubulake*, 220 F.R.D. at 219-20. *Zubulake*, therefore, asked for an instruction to the jury that it was allowed to infer that the evidence on those lost or destroyed tapes would have been favorable to her and harmful to her former employer. *Id.* at 219.

Zubulake held that three elements must be satisfied for the imposition of an adverse inference. The party seeking

the adverse inference must show: “(1) that the party having control over the evidence had an obligation to preserve it at the time it was destroyed; (2) that the records were destroyed with a ‘culpable state of mind’; and (3) that the destroyed evidence was ‘relevant’ to the party’s claim or defense such that a reasonable trier of fact could find that it would support the claim or defense.” *Id.* at 220. However, if the destruction was done willfully, then the party seeking an adverse instruction need not prove that the evidence was “relevant.” *Id.*

Notably, *Zubulake* concluded that the requisite “culpable state of mind” could include mere negligence. *Id.* The court further concluded that “[o]nce the duty to preserve attaches, any destruction of documents is, at a minimum, negligent.” *Id.* Thus, in effect, the first two requirements are really collapsed into one analysis – did the party have a duty to preserve the information. If it did and the information was destroyed, the first two requirements for an adverse instruction are satisfied.

Initially, *Zubulake* could prove only that the destruction of the e-mails was negligent and could not prove that “relevant” evidence was destroyed. Accordingly, at first, the court found that she was not entitled to an adverse inference. *Id.* at 222.

Later, however, new evidence came to light which established that despite counsel’s instructions to initiate a “litigation hold” on all relevant e-mails, certain e-mails had been deleted by several key players in the dispute. Some of these e-mails were retrieved and produced very late in the litigation, but others were irretrievably lost. *See Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422, 426-429 (S.D.N.Y. 2004).

In light of these new facts, the *Zubulake* court reconsidered its ruling relative to the adverse inference. Most important, the court held that merely issuing a “litigation hold” is not sufficient to satisfy the duty of preservation. *Id.* at 432. Rather, the party and counsel must affirmatively monitor the efforts to ensure compliance with the hold and

the retention of all relevant electronic data. *Id.* The court noted that to properly monitor compliance, counsel, in-house legal staff and the information technology staff should consult each other to make sure all sources of electronic data are identified and preserved. *Id.* In addition, the key players in the case should be consulted so that they have a clear understanding of the types of data that they should preserve and forward to counsel. *Id.*

Given the newly discovered lost evidence and the extreme delay in production of other evidence, the *Zubulake* court now found that the former employer’s conduct was willful. *Id.* at 436. This finding, by definition, resulted in the presumption that the lost evidence was “relevant.” *Id.* at 436. As a result, the court found that *Zubulake* had now satisfied the three requirements for an adverse inference instruction. *Id.* at 436-37. *Zubulake* was also granted permission to re-depose any witnesses she wanted at her former employer’s expense. *Id.* at 437.

Finally, the *Zubulake* court suggested a list of things counsel and legal staff should do to ensure compliance with discovery obligations and avoid such a sanction. First, they should issue a litigation hold as soon as litigation is anticipated and then re-issue that instruction on a periodic basis. *Id.* at 433. Second, legal staff should communicate with the key players to ensure compliance and make sure their means of preservation are sufficient. Key players should likewise be periodically reminded of the litigation hold. *Id.* at 433-34. Third, legal staff should instruct all employees to produce electronic copies of their active files and make sure that all back-up media is identified and stored for safe-keeping. *Id.* at 434.

B. Case Study: Mosaid

In *Mosaid*, the defendant continued with its normal e-mail retention policy, which called for the destruction of historical e-mails on a rolling basis. The defendant kept this retention policy in place, and continued to destroy e-mails on a rolling basis, even after the litigation was filed.

As a result, almost no relevant e-mails were retained or produced. *Mosaid*, 348 F. Supp. 2d at 333.

The *Mosaid* court required a four-part showing to adopt an adverse inference: (a) the e-mails were within the party's control; (b) there was actual suppression or withholding of the evidence; (c) the evidence suppressed or withheld was relevant to claims or defenses; and (d) it was reasonably foreseeable that the evidence would be discoverable. *Id.* at 336. The defendant in *Mosaid* argued that the "actual suppression" showing requires that the destruction be intentional. *Id.* at 337. According to that defendant, its destruction of the e-mails was not intentional, but was rather pursuant to its normal e-mail retention policy. The court quickly rejected this argument, explaining that "[w]hen the duty to preserve is triggered, it cannot be a defense to a spoliation claim that the party inadvertently failed to place a 'litigation hold' or 'off switch' on its document retention policy to stop the destruction of that evidence." *Id.* at 339. Thus, an adverse inference was adopted.

C. Case Study: Residential Funding

In *Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99 (2d Cir. 2002), the plaintiff delayed in producing its e-mail files and eventually tendered e-mail archive tapes to the defendant within days of the trial. *Id.* at 105. The plaintiff explained that the delay was caused by its own internal technology deficiencies and the fact that even an outside third-party vendor could not recover data from the archive tapes in a timely manner.

The defendants moved before the district court for the imposition of an adverse inference because of the discovery delays. The motion was denied, in large part because the district court concluded that the plaintiff had not acted with bad faith or gross negligence. *Id.* at 108. On appeal, the district court's order denying sanctions was vacated and the case remanded with permission for the defendant to file a new motion for sanctions under the guidelines set forth by the appellate court. *Id.* at 112 -13.

Three aspects of this case are important to consider. First, the Second Circuit clearly held that sanctions may be awarded for the mere delay in production of electronic data. The actual destruction of this data is not required for the award of sanctions. *Id.* at 110. Second, the appellate court rejected the idea that a showing of bad faith or gross negligence was required to award sanctions. Rather, "[t]he sanction of an adverse inference may be appropriate in some cases involving the negligent destruction of evidence because each party should bear the risk of its own negligence." *Id.* at 108. Third, the plaintiff argued that it did not have the necessary culpability in connection with the delay because it hired a third-party vendor to help retrieve the data and even the third-party vendor could not do so in a timely fashion. Even this argument was rejected, in part, because a different third-party vendor subsequently hired by the defendant was able to retrieve thousands of e-mails within days of obtaining the back-up tapes. *Id.* at 104, 111.

From these cases, it is abundantly clear that litigants must be very aggressive in preserving their electronic data. Merely issuing a litigation hold is not enough. The hold needs to be closely monitored to ensure compliance. And the legal staff must make sure to involve the information technology staff at a very early stage to make sure all of the potential sources of electronic data are quickly identified and isolated for preservation.

3. RESTRICTED USE OF EVIDENCE

A third possible sanction for the failure to preserve or produce electronic data is to restrict the use of that data. In *Thompson*, the defendant failed to preserve certain e-mails and also produced 80,000 e-mail records after the close of discovery and after a prior deadline set by the court. *Thompson*, 219 F.R.D. at 96. As a sanction for the late production, the court severely restricted the defendant's use of these e-mails. The defendants were prohibited from using (or introducing into evidence) at trial any of the 80,000 e-mail records. Moreover, the e-mails could not be used in the preparation of defense witnesses and/or by the defense to refresh the recollection of any defense

witnesses. Conversely, the plaintiff was allowed to use the e-mail records in any way it deemed fit – including in the cross-examination of defense witnesses. *Id.* at 104-05.

The *Thompson* court used a five-part test to determine the appropriate sanction: (a) the surprise to the party against whom the evidence would be offered; (b) the ability of that party to cure the surprise; (c) the extent to which allowing the evidence would disrupt the trial; (d) the importance of the discovery; and (e) the explanation of the non-disclosing party for its failure to provide the discovery. *Id.* at 103. This five-part test appears to be geared mostly to a situation where electronic data is produced very late in the litigation – likely after discovery and after depositions. It appears from the *Thompson* analysis that the key considerations are the prejudice caused by the late disclosure and the presence of a legitimate reason for the delayed disclosure. In all events, it is important to note that a mere delay in finding electronic data may very well result in the same type of sanction imposed when data is lost or destroyed.

Who Pays For All Of This?

Given the broad scope of discovery permitted relative to electronic data, one frequent question is not whether it must be preserved and produced in litigation – but who should pay for its retrieval and production. A complete analysis of this topic is beyond the scope of this article. However, we can summarize a few general rules. Most courts follow a presumption that the party in possession of the information must pay for its retrieval and production. *E.g., Zubulake*, 217 F.R.D. at 317. However, courts will consider shifting the cost of retrieval and production to the party requesting the data if that request imposes an “undue burden.” *Id.* at 318. This term is quite vague, but generally is determined based upon a balancing of the cost of retrieving and producing the information versus the likely benefit of that information given the specifics of the case. *Id.* See also *Wiginton v. CB Richard Ellis, Inc.*, 229 F.R.D. 568 (N.D. Ill. 2004) (eight-factor test).

Conclusion

As we have noted throughout this article, the actual duties relative to electronic data will be decided in large part based upon the specific facts of a case. However, from the general discussion above and the case law summarized above, there are three key points to keep in mind at all times.

First, as soon as a legal dispute becomes apparent, legal and information technology personnel should meet to determine the universe of potential sources of electronic data that is possibly relevant to the dispute.

Second, legal and information technology staff should immediately meet with the “key players” in the potential dispute to determine if there are any off-line or unique storage methods used by those key players. For example, if the key players frequently use their home computer for work or store data on mobile communication devices, those sources should be identified.

Third, all of the potential sources of electronic data identified in steps one and two should be frozen by a litigation hold. Regardless of retention/destruction policies, all data in those sources as of the date a dispute is apparent should be preserved. And all future communications in any way relevant to the dispute should also be isolated and preserved. This “litigation freeze” must also be aggressively monitored to ensure full compliance.

Once these three steps are taken, it then becomes a very fact specific process to determine the best way to store the information with minimal disruption to other day-to-day activities; the best way to make this data available to your own counsel; and the best way to make this data available to opposing counsel, etc.

In closing, the changing technology and discovery rules ensure that the issue of electronic data discovery will be a crucial issue subject to dispute and change in the coming years. It is important for all attorneys to be familiar with the potential sources of electronic data to ensure that the process of gathering and producing this information is complete. It is also important for in-house legal staff to be on the same page as the information technology staff to ensure that they can respond in a coordinated and effective way when the threat of litigation arises.

ABOUT THE FIRM

Novack and Macey LLP is a litigation firm that concentrates in complex commercial matters, including matters involving banking, contracts, class actions, creditors' rights, energy, RICO, securities, business torts, real estate, partnerships and close corporations, employment, unfair competition and antitrust, insurance coverage and environmental issues.

Novack and Macey LLP prides itself on being creative while providing sound, practical and cost effective advice and representation. Please contact us if you have a legal problem that you wish to discuss. *The Litigation Review* is a periodic publication of Novack and Macey LLP, and addresses legal issues that impact commercial litigation. The publication is edited by Mitchell L. Marinello and Monte L. Mann.

We are interested in providing our newsletter to as many readers as would find the information useful. Please let us know of any of your colleagues who would like to receive *The Litigation Review*. Such requests and any comments may be sent to the editor at: mmarinello@novackandmacey.com or mmann@novackandmacey.com.

Issues of *The Litigation Review* may be downloaded from our web site, www.novackandmacey.com, using Adobe Acrobat.

Novack and Macey LLP provides this newsletter for informational purposes only. The information contained in this newsletter is not legal advice, and it is not intended to and does not create any attorney-client relationship with the recipient. Readers should consult with a lawyer before acting in reliance on any such information. Although Novack and Macey LLP has attempted to make the information in

this newsletter as timely and as accurate as possible, there may be inaccuracies due to, among other things, the fact that laws, and their interpretations, constantly change and vary from jurisdiction to jurisdiction. Novack and Macey LLP assumes no responsibility, and expressly disclaims all liability, for errors or omissions in, and use or interpretation by others of, any information contained in this newsletter.

CONTACT INFORMATION

Novack and Macey LLP
100 North Riverside Plaza
Chicago, Il 60606-1501
t 312 419 6900
f 312 419 6928
www.novackandmacey.com