

SPOLIATION OF DIGITAL EVIDENCE: A CHANGING APPROACH TO CHALLENGES AND SANCTIONS

STEVEN W. TEPPLER
AUTHOR

After the Zubulake decision, businesses now have a duty to preserve electronic evidence or face sanctions. This article discusses the obligations of this decision for businesses, including forensic and antforensic software to assist in managing data.

SPOILIATION OF DIGITAL EVIDENCE

A CHANGING APPROACH TO CHALLENGES AND SANCTIONS

By Steven W. Teppler

Spoliation is “the destruction or significant alteration of evidence or the failure to preserve the property for another’s use as evidence in pending or reasonably foreseeable litigation.”¹

Evidentiary spoliation is a concept that is neither new nor infrequently encountered in judicial proceedings.² Historically, there has been little, if any, judicial toleration of documentary spoliation, and the courts’ gaze upon spoliators in the past has not been kind:

It is because of the very fact that the evidence of the plaintiff, the proofs of his claim . . . have been destroyed, that the law, in hatred of the spoiler, baffles the destroyer, and thwarts his iniquitous purpose, by indulging a presumption which supplies the lost proof, and thus defeats the wrong-doer by the very means he had so confidently employed to perpetrate the wrong. . . .

Numerous instances are given in the books of the like application of the rule, where it is held that spoliation of documentary evi-

dence being proved against a defendant, that thereby he is held to admit the truth of the plaintiff’s allegations; and this upon the ground that the law, in consequence of the fraud practiced, in consequence of the spoliation, will presume that the evidence destroyed would establish the plaintiff’s demand to be just.³

More recent court decisions have tended to support this approach. In citing the *Pomeroy* case (and its invocation of what the court sees as “Old Testament” fury), a 2003 decision from the United States District Court for the Southern District of New York succinctly states that: “It has long been the rule that spoliators should not benefit from their wrongdoing, as illustrated by that favorite maxim of law, *omnia presumuntur contra spoliaterum*.”⁴ Indeed, it can be generally assumed that evidentiary spoliation issues are not new, and have in some manner plagued the bench and the bar for as long as evidence has been used in judicial proceedings.

The sanctions for spoliation of evidence are typically decided on a case-by-case basis. The menu of remedies for spoliation hinges in large part upon the

degree of culpability or intent of the spoliating party or counsel. Penalties generally start with the imposition of monetary sanctions, but can also result in an adverse instruction to a jury, or even a default judgment or dismissal where a court finds that there has been intentional, rather than negligent, activity by the offending party or counsel.

Courts generally have wide latitude to impose sanctions for spoliation. The range of sanctions—for-spoliation Federal Rules of Civil Procedure are succinctly stated in the *Pastorello* decision:

Under the Federal Rules of Civil Procedure, a court can sanction any “party that without substantial justification fails to disclose information required by Rule 26(a) or 26(e)(2),” and “[i]n addition to requiring the payment of reasonable expenses, including attorneys fees, caused by the failure, these sanctions may include any of the actions authorized under Rule 37(b)(2)(A), (B), and (C) and may include informing the jury of the failure to make the disclosure.” Fed. R. Civ. P. 37(c). The authorized sanctions under Rule 37(b) consist of: an order estab-

Steven W. Teppler is an attorney, inventor, and the CEO of TimeCertain, LLC, an information security solutions company in Sarasota, Florida.

lishing facts related to the discovery abuse, prohibiting the disobedient party from supporting or opposing related claims and defenses, striking out pleadings or parts thereof, or entering a default judgment against the disobedient party.⁵

The flexibility of remedies for spoliation is reflected in the language used by the Second Circuit in *West*: “the applicable sanction should be molded to serve the prophylactic, punitive, and remedial rationales underlying the spoliation doctrine.”⁶

With this framework in mind, we now turn to spoliation issues as they relate to computer-generated information.

The Shift in Specie of Evidence from “Physical” to “Digital”

Until relatively recently, the bench and the bar have in the main focused on evidence that is either physical in nature, or evidence upon which has been *first* written or printed out on some specie of paper and ink.

Currently, however, more than 90 percent of all source information today is generated electronically.⁷ With the introduction of computer-generated information as source of most evidence, both the prelitigation as well as the litigation landscape has been permanently altered. Moreover, and depending upon one’s point of view, the December 2006 amendments to the discovery provisions of the Federal Rules of Civil Procedure either presage or memorialize the importance of obtaining electronically generated information, rather than “paper print-outs,” as evidence.⁸

What should be clear to both lawyers and the courts is that most litigated information will therefore also be digital in source as well as in nature. Perhaps the most significant adverse consequence resulting from the onslaught of computer-generated information into the discovery and trial process is the introduction of spoliation issues and potential challenges uniquely inherent to computer-generated information used, or attempted to be used, as evidence.

Why Computer-Generated Evidence Is Different

Computer-generated information, or digital data, is comprised of binary digits (zeroes and ones).⁹ Digital data were created with the intent to allow ease of manipulation, substitution, and deletion by those with control over the data.

Electronic data content can be created, changed, substituted, or deleted by human hands, often without ways to detect who made the changes and when.¹⁰ The challenge presented by electronic (or digital) data from an evidentiary perspective is that they are, by design, ephemeral in nature. These ephemeral binaries, or zeroes and ones, are intended by design to be manipulated, and further intended by design to be manipulated in a manner that is either undetectable or difficult to detect. From a litigation perspective, this heightened ephemerality-by-design reduces the reliability of any digital information offered as evidence.

Spoliation in the Digital Evidence Universe

Examples of spoliation techniques abound. Digital evidence may simply be electronically deleted, or the media that store them can be physically destroyed. Digital information can be undetectably backdated and modified, altered, or deleted, resulting in evidence that is created after-the-fact, altered after-the-fact, or backdated after-the-fact.

Using the Second Circuit’s analysis in *West*, digital evidence spoliation will occur where a party or a party’s counsel significantly alters or destroys computer-generated evidence, or fails to preserve such computer-generated information “for another’s use as evidence in pending or reasonably foreseeable litigation.”¹¹

What lawyers and jurists across the nation are now witnessing is the drawback of a tsunami. From an evidentiary perspective, computer-generated information either comprises (or will comprise) the “source” or “original” evidence in most litigation. The ever-increasing number of litigated matters involving electronic discovery will necessarily result in waves of digital evi-

dence that will be offered, examined, challenged, and perhaps introduced into evidence in these matters.

That said, that specie of evidence characterized by the Federal Rules of Civil Procedure as “electronically stored information” still has as its origination the binary sets of zeroes and ones that are highly susceptible to undetectable, or nearly undetectable manipulation. This heightened ephemerality of computer-generated information, with its correspondingly reduced degree of reliability, creates spoliation capabilities and issues inherently unique to computer-generated evidence. Moreover, the ease with which such tools may be deployed rather handily provides powerful spoliation tools to both parties and their counsel. The frailty in reliability of this new specie of evidence compels in turn a new more nuanced approach to both claims of spoliation as well as judicial response to these claims.

Zubulake v. Warburg, LLC

The landmark and perhaps seminal spoliation decision set in the computer-generated information arena is the various opinions arising from *Zubulake IV*, in which sanctions were sought for failure to preserve electronic evidence.¹² In perhaps the most well-reasoned set of opinions discussing the ramifications of digital evidence spoliation, the court in *Zubulake IV* first imposed sanctions of redepositions for failure to preserve all relevant backup tapes, and then, in a follow-on decision, imposed the sanction of adverse inference instruction to be given for willful destruction (deletion) of relevant email.¹³ In finding sufficient basis for an adverse inference instruction to be given to the jury, the court ruled that a presumption of relevance arose where the spoliation was willful.¹⁴

Post-*Zubulake* Spoliation Decisions

Recent decisional authority illustrates what appears to be an increasingly hostile judicial reaction to spoliation of digital evidence. In a recent case from the U.S. District Court for the Western District of North Carolina, the court

found sufficient evidence to direct an adverse inference instruction to the jury at trial because the plaintiff “discarded the computer well after she had retained counsel and filed her EEOC charge” and because “the computer contained evidence directly related to her lawsuit against Target.”¹⁵ In this case, the plaintiff had discarded her computer, which contained email and other data relevant to her claims, because it had “crashed.” Further, the plaintiff did not attempt to repair the computer or to have it examined to determine whether it could be repaired.

In a Kansas bankruptcy matter, the court found that the defendant/debtor, who was also a lawyer, had digital evidence. In this case, the court found that debtor was running a data (and digital evidence) “wiping” utility called “GhostSurf” on his computers and that he was obligated to disengage the wiping software to preserve the electronic evidence.¹⁶ The court further found that, once the duty to preserve attached, the debtor was “required to suspend his routine document destruction practices, be it the deletion of e-mails or the operation of wiping software to prevent recovery of the electronic evidence. If the electronic evidence was stored other than on the hard drives, Krause had a duty to preserve any such storage devices and any backup or copied files.”¹⁷

The various options backdating revelations involving more than 100 publicly traded companies also provide potential claims of spoliation by backdating computer-generated information. In these instances, the timing of equity option issuances to company executives (as well as the “strike price” associated with such grants) were altered by company executives in such a way as to either maximize profit, or minimize the tax consequences. Perhaps the most illustrative example of backdating is that done by the former general counsel of McAfee, Inc., whose indictment alleges that he caused McAfee controller to fabricate the grant date and change the option price to make the options grant more

favorable. Ironically, and in what appears to be an attempt to cover his tracks, the former McAfee general counsel then had the controller terminated for backdating options grants.¹⁸ Utilizing the Second Circuit’s approach in *West*, the potential spoliation argument that might have been asserted here is that the criminal acts of fraudulently altering computer-generated information resulted in the “destruction or significant alteration of evidence or the failure to preserve the property for another’s use as evidence in . . . reasonably foreseeable litigation.” Moreover, as articulated by the court in *Zubulake IV*, spoliation may occur where a party fails to preserve evidence that “may be relevant to future litigation.” Under this analysis, the failure of McAfee’s former general counsel to preserve the unaltered and nonbackdated computer-generated option grant data would constitute a spoliation event.

Control and Detectability

The common thread of “control” runs through the above-mentioned examples of digital evidence spoliation. In each case, the party or party’s attorney accused of spoliation exerted *control* over the computer system that generated the computer-generated information, or control over the computer-generated information itself. The court in *Zubulake V* takes note of this and states that:

The spoliation of evidence germane “to proof of an issue at trial can support an inference that the evidence would have been unfavorable to the party responsible for its destruction.” A party seeking an adverse inference instruction (or other sanctions) based on the spoliation of evidence must establish the following three elements: (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 that claim or defense.”¹⁹

A compelling argument may be made to the effect that presence of “control” takes on even greater significance as it relates to the generation of digital evidence. This increased importance is the direct consequence of (1) computer-generated information’s inherent ephemerality, and (2) the ease with which alterations or deletions of computer-generated information may be made undetectable, or nearly impossible to detect.

That the obligation to preserve evidence inures to both a party as well as a party’s counsel is undisputed, but the capability to exert control over computer-generated information may lie with both a party’s counsel as well as the party itself. Perhaps the most striking example to date of a counsel-in-control is that of the now-former codefendant’s counsel in a pending consumer fraud action in Washington State.²⁰ The *Minneapolis Star Tribune* reported on June 4, 2007, that defendant Best Buy’s lead counsel admitted to falsifying and deleting email and email attachments, giving rise to a potential (and potentially disastrous) spoliation claim.²¹ It may be readily assumed that the lawyer for Best Buy had fairly typical (and high) supervisory powers in the handling of discovery matters for his client. These powers in all likelihood also included review, redaction, and production of email and attachments. In order to have deleted and redacted the affected email and attachments, Best Buy’s lawyer must have had and exerted control over the email and attachments sufficient to perform these actions. What is perhaps even more significant is that, absent the revelation by counsel, it is extremely unlikely that this spoliation would ever have been discovered.

In the McAfee, Inc., options backdating matter, the former general

counsel of publicly traded McAfee, Inc. exerted sufficient control over the enterprise computer system (and IT personnel) generating the options grant information sufficient to commit spoliation of digital evidence. In this instance the former general counsel exerted control over McAfee's then-chief financial officer to alter or fabricate digital evidence.²² In *Teague v Target*, the plaintiff had complete control over her computer and the digital evidence generated by it, and chose to discard the computer, containing relevant and material evidence, even after she commenced her litigation against defendant Target Stores.²³ In *In re Krause*, the debtor/bankrupt, who was also a lawyer, also exerted complete control over his computer system as well as the data generated by it.²⁴

These cases underscore the complete malleability of computer-generated information by a party or by counsel who exerts control over either the digital evidence, or the computer system that generated the digital evidence.

Forensics and Antiforensics

The century just past has seen the evolution of ever more accurate forensic testing capabilities in determining both the provenance of evidence, as well as likelihood of spoliation. These tests have been further refined to encompass custodial protections to prevent or detect potential spoliation occurring either before, or after litigation has commenced. In a paper-and-ink world, such tests might include chemical testing of paper, of ink to determine age, or perhaps to determine the date of manufacture of watermarked paper, or date of first commercial introduction of ink. In a case from the United States District Court for the Northern District of California, a plaintiff-inventor seeking to enforce a patent claim had his patent invalidated when, following a forensic analysis involving the testing of the chemical composition of the ink used to write his inventor's logbook, it was determined that fraudulent material was later added to a once genuine notebook.²⁵ Here, it was the ink used to create the fraudulent entry that

exposed the attempted spoliation. After investigation and testing, it was determined that the ink was introduced into commerce *after* the date of the alleged entry in plaintiff's inventor's notebook.

Numerous digital data forensic tools, such as enCase, have been introduced and are in widespread commercial use. The enCase application generally creates a mirror image of every sector of a computer's hard drive, with, it is claimed, no change to the hard drive that is imaged. Such forensic tools perform hardware- or software-based disk imaging and analysis (with or without write blocks), deleted file recovery, password cracking, and other tasks. These forensic tools can help to determine actions taken on computer hard drives that might indicate fraudulent creation, modification, or deletion of digital evidence, all of which can aid in the detection of digital evidence spoliation. The National Institute of Science and Technology (NIST) has commenced a program by which such tools may be certified to accomplish what they claim.²⁶

Nonetheless, and largely due to the ephemeral nature of digital data, numerous antiforensic tools have been developed to defeat the testing efficacy of such forensic tools. These tools are designed to enable undetectable access and control over a computer system.²⁷ One of these tools is a program named Timestomp. Timestomp permits the manipulation of metadata (critical to computer forensic examinations). Metadata, or data about data, includes files logs, and the times that a files or file system was accessed, created, modified, viewed, or deleted. Essentially, Timestomp permits what may be the *crème de la crème* of spoliation events: recreating history by digital data manipulation. Another program named Transmogrify allows an attacker or person in control to undetectably change information in a file header.

Legitimate forensic tools may also have antiforensic features. For example, a computer hard drive imaging product (hardware- or software-based) should offer to image an entire hard drive, in a sector-by-sector and bit-by-bit manner, including deleted files (which are really never really deleted until overwritten)

and file slack space. Some imaging programs do not perform a sector/bit routine, and will not recover either deleted files or information contained in slack space. The choice of such an imaging program can lead to the assertion of a spoliation claim against a party or its counsel, because the imaging program deleted or failed to copy "all" the electronic evidence requested.

These antiforensic programs are either designed or sport a feature that enables spoliation. The consequence of these recent developments is that a challenge of spoliation may be made even in the face of an assertion by the alleged spoliating party that "we used computer forensic tools to comply with production requests."

The Assertion of "Global Taint" in Determining Sanctions for Spoliation

Where spoliation of computer-generated information is determined to have occurred, a natural and logical claim of "global taint" may now be asserted by the party disadvantaged by the alleged spoliation, and the aggrieved party should move for relief by way of requesting either an adverse instruction, or a default judgment, or dismissal. The taint should be challenged as global because the spoliation of one portion of the computer-generated information produced in discovery, or offered as evidence in all likelihood inures in turn to all other digital evidence produced by the spoliating party or its counsel. Using currently deployed technologies, it would also be extremely difficult to ascertain the negative, i.e., that the rest of the data set or data sets provided by the spoliating party were pristine and not spoliated. This basis for assertion of "global taint" is supported by the ephemerality-by-design of computer-generated information, the ease with which such information may be undetectably and fraudulently created, deleted or altered, and the ability to carry out these actions by those who have access and control over the subject computer-generating system or digital data. As digital evidence is gathered either prior to or after the commencement of litiga-

tion, it will pass through (and be under the control of) the hands of both the party as well as the party's counsel. As illustrated by the *Odom v. Microsoft et al.* (the Best Buy case), *Teague*, and *In re Krause* litigation, a party or its counsel may exert sufficient control over computer-generated evidence to cause spoliation by undetectable or nearly undetectable alteration, deletion, or destruction or fabrication. A party so disadvantaged by another party's (or counsel's) spoliation may never be able to obtain, and the court may never be capable of considering, the true source digital evidence, with any assurance that it has, over time, not been managed by a party or counsel in control, even with assistance from current state-of-the-art forensic testing and examination. (Accordingly, and in this author's opinion, the stronger consideration of application of adverse instructions, defaults, or dismissals as sanctions for spoliation may in these cases be appropriate and should be granted for both their deterrent as well as their remedial value.)

Lowering the Bar for Successful Assertions of Spoliation of Digital Evidence

Where the spoliation of digital evidence is so easily undetectable, and where antiforensic measures may be taken to forever prevent such detection, a party alleging spoliation will invariably run up against the argument offered by the alleged spoliator (or by the court) to the effect that such allegations are no more than mere conjecture or speculation, unsupported by facts. Moreover, pleas will be made to the court to take no action absent something approaching clear evidence of wrongdoing. It is this

author's position that the problem with this approach is that it fails to take into account that a well-executed digital evidence spoliation scheme will, in all likelihood, never be discovered absent a confession similar to that undertaken by Best Buy's former counsel in *Odom v. Microsoft et al.* In a litigation universe where digital evidence may well be the *only* evidence, where spoliation of digital evidence is so easily carried out by those in control, and where the likelihood of detection is so low as to be nearly impossible, a court should initiate additional and intensive inquiry into both control as well as the custody of computer-generated information. ♦

Endnotes

1. *West v. Goodyear Tire & Rubber Co.*, 67 F.3d 776, 779 (2d Cir.1998).
2. *See, e.g., Pomeroy v. Benton*, 77 Mo. 84, 86, 1882 WL 9684 (Mo. 1882)
3. *Pomeroy v. Benton*, 1882 WL 9684 at *12 [Internal citations omitted].
4. *Pastorello v. City of New York*, 2003 WL 1740606 (S.D.N.Y. 2003).
5. *Id.*
6. *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 779 (2d Cir.1999).
7. PETER LYMAN & HAL R. VARIAN, *How Much Information?* at www.sims.berkeley.edu/how-much-info-2003 (last visited July 4, 2007).
8. *See, e.g., FED. R. CIV. P. RULES* 16(b)(5); 26(a)(1)(B), 34(a),(b); 37; 45(a)(1)(C).
9. Bruce H. Nearon, Jon Stanley, Steven W. Tepler, and Joseph Burton, *Life After Sarbanes-Oxley: The Merger of Information Security and Accountability*, 45 JURIMETRICS J. 379-412, at 387 (2005).
10. *Id.*
11. *West v. Goodyear Tire & Rubber*

- Co., 67 F.3d at p. 779.
12. *Zubulake v. UBS Warburg, LLC*, 220 F.R.D. 212 (S.D.N.Y. 2004).
13. *Zubulake v. UBS Warburg, LLC (Zubulake V)*, 229 F.R.D. 422 (S.D.N.Y. 2004).
14. *Id.*
15. *Teague v Target Stores, Inc.*, at *1. *Teague v. Target Corporation d/b/a Target Stores, Inc.* 2007 WL 1041191 (W.D.N.C. April 2007).
16. *In re Krause*, 367 B.R. 740 (Bankr. D. Kan. June 2007).
17. *Ibid*, at pp. 758-59.
18. *U.S. v. Roberts*, CR 07-0100, U.S. District Court for the Northern District of California, Indictment Filed February 27, 2007.
19. *Zubulake V*, 229 F.R.D. at 430 [Internal footnotes and citations omitted].
20. *Odom et al., v. Microsoft Corporation, Best Buy Co., Inc. et al.*, No. 04-2-10618-4 SEA (Super. Ct. King County 2004).
21. Steve Alexander, *Best Buy Attorney Falsified Emails*, StarTribune.com, June 4, 2007.
22. *U.S. v. Roberts*, CR 07-0100, U.S. District Court for the Northern District of California, Indictment Filed February 27, 2007.
23. *Teague v. Target Corp., d/b/a Target Stores, Inc.*, 2007 WL 1041191 at *2.
24. *In re Krause* 367 B.R. 740 at pp. 754, 768.
25. *See, e.g., Aptix Corp. v. Quickturn Design Sys., Inc.*, No. C 98-00762 WHA, 2000 U.S. Dist. LEXIS 3408, at *71 (N.D. Cal. June 14, 2000).
26. *Computer Forensics Testing Tool, Information Technology Laboratory*, www.cftt.nist.gov/project_overview.htm, last viewed July 5, 2007.
27. *See SCOTT BERINATO, The Rise of Antiforensics*, CSO MAG., June 2007.

Spoliation of Digital Evidence: A Changing Approach to Challenges and Sanctions

**First published in Vol. 4, No. 2, Fall 2007 of *SciTech Lawyer*,
a publication of the Section of Science & Technology Law.**

About the Section of Science & Technology Law

The mission of the ABA Section of Science & Technology Law is to provide leadership on emerging issues at the intersection of law, science, and technology; to promote sound policy and public understanding on such issues; and to enhance the professional development of its members.

<http://www.abanet.org/scitech>

About ABA Publishing

ABA Publishing is a division of the American Bar Association (ABA), responsible for providing professional publishing guidance to both the association and its members. Our legal publications support professional excellence and greater understanding of the law. We publish approximately 100 law books per year as well as approximately 75+ magazines, newsletters, and journals in numerous specialized areas of the law.

Our law books provide the best practice tips and pointers, sample forms and language, and professional legal guidance from experienced practitioners and are available in a variety of formats, including print, PDF, audio, and CD-ROM. Our authors and editors are outstanding professionals who are active in their fields. Experts rigorously review our products to ensure the highest quality information and presentation.

Articles

Individual articles are available as PDF downloads at www.abanet.org/abastore/index.cfm

For customer service, call 1-312-285-2221

Monday–Friday, 7:30–5:00 CST