



AccessData Corporation

The Collection Process: Collecting Evidence or Collecting Sanctions?

White Paper



AccessData®
A Pioneer in Digital Investigations Since 1987

Documents and other information are central to every legal matter—even for those matters that do not involve litigation. For matters involving litigation (even potential litigation), an extra duty—preservation—is imposed upon the party.

¹ Spoliation of evidence, when there is a duty to preserve it, can prompt a court to impose sanctions on you (the attorney) and/or your company. Sanctions are often monetary,² but other sanctions include: the striking of pleadings,³ default judgment,⁴ dismissal of the case⁵ or an adverse inference.⁶

The duty to preserve implies two subsequent actions, namely the identification of the relevant information, and the collection of that information for review and possible production/presentation. Thus, for each case the attorney must find the relevant information and decide how to preserve it. The preservation of the information, however, can be affected by how the information is collected. Consequently, a sanction-averse attorney would do well to acquaint him/herself with their collection options.

There are many “right” and some “wrong” ways to collect and to preserve potentially relevant evidence. No matter what, however, the attorney and/or client will need to take some action and that action will likely entail some software application in order to take advantage of any safe harbor provisions.

⁷ What constitutes a right or a wrong collection process can be subjective, with the last word belonging to a judge. From the attorney's standpoint, there are only two main varieties of collection procedures: copy/sequester and in-place hold (also referred to as hold in-place). Each procedure has benefits and shortcomings. More importantly, each procedure has a different potential for sanctions by a court.

Copy/Sequester

Attorneys prefer the copy/sequester method because it mirrors sound forensic guidelines promulgated by many law enforcement agencies, such as the U.S. Department of Justice.⁸ The copy/sequester method doesn't make a single copy of the original document. Instead, two copies are typically made. Experts utilize the second copy (called a “working copy”) for analysis. The first copy is left undisturbed and can be used to obtain working copies of the document if the review/examination process corrupts the original working copy.

If there is a question regarding the integrity of the document, the question can be resolved by reference to the first copy in a manner easily defensible to a court.⁹ The copy/sequestration method, if done with a reliable, industry-standard forensic software application, can make an exact copy the document itself and the associated metadata while leaving the original document in place for further use by the client. Remember, if not done correctly, the process of copying can result in spoliation of the evidence.

In the past, some attorneys were concerned whether the copied electronic files adhered to the best evidence rule.¹⁰ This isn't a problem in today's computerized legal environment. Recall that the best evidence rule was promulgated in the 19th Century, when it was difficult to make copies of a document at all, let alone with precision. However in the 21st Century, making precisely identical copies of an electronic document is trivial and reliable with the right software. Because precisely identical copies of electronic documents and their associated metadata can be readily made, creating authenticatable copies of ESI—if done properly—does not subject the attorney to a sanctions motion for spoliation of evidence.

While copying electronic documents and their associated metadata can be readily accomplished, the attorney needs to ensure that the copying is done properly. Simply making copies by burning CDs, copying files to thumbdrives or "ghosting" may seem adequate, but unless you are very careful, you will likely alter (irreparably) some of the metadata associated with the original file, thus tampering with the evidence.¹¹ In some cases, the altering of such metadata has resulted in sanctions.¹² It is always better to use a computer forensic tool that is designed to preserve all of the evidence when making a copy using default settings.

Sequestration of the copied evidence is the obvious second step in the method. Sequestration can take many forms, such as locking the hard drives containing the copies of the evidence in a secure locker in the legal department, or storing the information at an offsite location. There is no objective standard for the sequestration step, although attorneys should exercise reasonable judgment. The key is separating the first (archive) copy of the information from both the original copy and the working copy used by attorneys and experts, and maintaining the security of the various copies. This ensures that there is a source where, if all else fails, a precise copy of the original evidence is available to remedy problems.

In-Place Hold

As the name suggests, in-place hold allows the original electronic documents to remain where they are. The benefits are obvious. The attorney doesn't have to disrupt access to his or her client's data during a copying process. However, in order to adhere to litigation hold notices or other preservation considerations, the attorney must impose some safeguards so that the original electronic documents are not disturbed. This can be accomplished by forcing the client to save new/updated documents to another location. Unfortunately, not only does the "copy new/updated files to a new place" method disrupt the client's normal business operations, that method also requires strict cooperation by the client and their employees. Worse, to avoid frustration, some employees may not adhere to the terms of the litigation hold, and destroy the evidence.¹³

Circumvention of the in-place hold methodologies, particularly those employing agent-less software applications, rely upon features¹⁴ of the underlying operating system.¹⁵ However, employees using tools readily available on the Internet can modify the privilege levels of relevant files and thus tamper with the evidence.¹⁶ Worse, even after software guards have been implemented, some custodians have been known to destroy the machine containing the evidence.¹⁷

While the Federal Rules do not preclude the in-place hold methodologies, "[c]ourts may consider the actions taken by counsel to ensure compliance with a party's preservation obligation."¹⁸ Indeed, the Court in *Hawaiian Airlines* noted that the defendant had alternatives to the in-place hold scheme that they had adopted, and sanctions were appropriate because the collection/sequestration option was not taken.¹⁹ The Sedona Conference has recently noted the need for quality assurance as part of the attorney's duty.²⁰ Indeed, the trend is to impose a duty on the attorney to require a certain level of quality assurance for the operations performed under his or her direction.²¹

Finally, one may question whether storing new/updated copies of the original documents in a different location is any less trouble than the copy/sequester method because, in both cases, there are two sets of documents in two locations. Wouldn't it have been

simpler to make a copy of the original set of documents and allow the client to continue using their machines in the normal fashion?

What Can Happen When Things Go Wrong?

If the “in-place hold” method fails for some reason, the requesting party can file a motion under Rule 34(a)²² and ask the Court to require the responding party to provide access to their system to the requesting party’s forensic expert or to a Court-appointed special master.²³ If there is evidence of spoliation, sanctions could be imposed on the producing party and their attorneys.²⁴

Under the copy/sequester method, about the only thing that can go wrong is the mechanical failure of the device containing the sequestered data. Such failures do happen.²⁵ However, no court has ever held it against an attorney or party when a mechanical failure outside the control of the attorney or client occurs.

Conclusion

Because employing the copy/sequester method reduces the potential for sanctions against the attorney and the client, most attorneys when faced with a choice will avoid the “in-place hold” method for preserving electronically stored information.

About AccessData®

AccessData has pioneered digital investigations for more than twenty years. Its automated, in-house eDiscovery solution allows users to identify, collect, forensically preserve, process, deduplicate and produce electronically stored data. It allows users to collect from laptops, desktops, databases, servers, email and more than 30 popular structured data repositories. Additionally, AccessData eDiscovery enables large-scale auditing to detect data leakage and files that aren’t in compliance with an organization’s retention policies. For more information visit: www.eDiscoveryWithAccessData.com

¹ "The duty to preserve evidence '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.'" *Acorn v. City of Nassau*, 2009 WL 605859 at 2 (E.D.N.Y. March 9, 2009) citing *Zubulake v. UBS Warburg LLC ("Zubulake IV")*, 220 F.R.D. 212, 216 (S.D.N.Y.2003) (which quoted *Fujitsu Ltd. v. Federal Express Corp.*, 247 F.3d 423, 436 (2d Cir.2001)). "Once the duty to preserve arises, a litigant is expected, at the very least, to 'suspend its routine document and retention/destruction policy and to put in place a litigation hold.'" *Id.*, citing *Zubulake IV*, 220 F.R.D. at 218; and also *Doe v. Norwalk Cmty. Coll.*, 2007 U.S. Dist LEXIS 51084, at *14 (D. Conn. July 16, 2007) (a party needs to take affirmative acts to prevent its system from routinely destroying information).

² See, e.g., *Kipperman v. Onex Corp.*, 2009 WL 1473708 (N.D. Ga. May 27, 2009) (\$1,022,700 in monetary sanctions levied against the defendant for "a textbook case of discovery abuse.")

³ FRCP Rule 37(b)(2)(iii): "striking pleadings in whole or in part". See, e.g., *Chanel Components, Inc. v. Am. II Electronics, Inc.*, 915 So. 2d 1278 (Fla. Dist. Ct. App. 2005) (striking of pleading considered, but not imposed by the Court).

⁴ FRCP Rule 37(b)(2)(vi): "rendering a default judgment against the disobedient party". See, e.g., *Gutman v. Klein*, 2008 WL 4682208 (E.D.N.Y. Oct 15, 2008) (Magistrate Judge recommended default judgment in favor of plaintiff, plus attorneys fees); *Atlantic Recording Corp. v. Howell*, 2008 WL 4080008 (D. Ariz. Aug. 29, 2008) (default judgment warranted after "brazen destruction of evidence").

⁵ FRCP Rule 37(b)(2)(v): "dismissing the action or proceeding in whole or in part" See, e.g., *Kvitka v. Puffin Co., LLC*, 2009 WL 385582 (M.D. Pa. Feb. 13, 2009) (all of plaintiff's claims were dismissed, and an adverse inference instruction awarded to defendant's cross-claims after plaintiff intentionally discarded her laptop in spite of a duty to preserve it).

⁶ See, e.g., *Smith v. Slifer Smith & Frampton/Vail Assocs. Real Estate, LLC*, 2009 WL 482603 (D. Colo. Feb. 25, 2009) (Despite lack of evidence of a "smoking gun," the Court awarded an adverse inference against the defendant because documents were destroyed well after the litigation hold notice was put in place.)

⁷ The safe harbor provisions are identified in FRCP Rule 37(e). See, e.g., *Gipetti v. UPS, Inc.*, 2008 WL 3264483 (N.D. Cal. Aug. 6, 2008) (Plaintiff's motion for sanctions were denied in view of a safe harbor provision because the documents that were destroyed were done so in accordance with the company's document retention policy and there was no apparent relevancy of those documents to the case given the Plaintiff's cause of action).

⁸ See, e.g., "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations," Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice, July 2002 at p. 53, available at <http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.pdf>. Judge Scheindlin in *Zubulake V* arguably endorsed elements of the copy/sequestration method when she set forth three actions that counsel should take in conjunction with the litigation hold, one of which was: "Finally, counsel should instruct all employees to produce electronic copies of their relevant active files. Counsel must also make sure that all backup media which the party is required to retain is identified and stored in a safe place." *Zubulake v. UBS Warburg*, 229 F.R.D. at 422, 434 (S.D.N.Y. July 20, 2004) (emphasis added).

⁹ The integrity of the copy can be verified by comparison to "hash values" using a cryptographic function, such as the Message-Digest algorithm "MD5". See, e.g., *Xpel Techs. Corp. v. Am. Filter Film Distribs.*, 2008 WL 744837 (W.D. Tex. Mar. 17, 2008) ("all images and copies of images shall be authenticated by generating an MD5 hash value verification for comparison to the original hard drive."); *Bro-Tech Corp. v. Thermax, Inc.*, 2008 WL 724627 (E.D. Pa. Mar. 17, 2008); *Creative Sci. Sys., Inc. v. Forex Capital Mkts., LLC*, 2006 WL 870973 (N.D. Cal. Apr. 4, 2006) (Unpublished).

¹⁰ The best evidence rule is also "referred to as the 'Original Writing Rule', because it does not mandate introduction of the 'best' evidence to prove the contents of a writing, recording or photograph, but merely requires such proof by an 'original,' 'duplicate' or, in certain instances, by 'secondary evidence'—any evidence that is something other than an original or duplicate (such as testimony, or a draft of a writing to prove the final version, if no original or duplicate is available." *Lorraine v. Markel Am. Ins. Col.*, 241 F.R.D. 534, 2007 U.S. Dist. LEXIS 33020 (D. Md. May 4, 2007) citing FED. R. EVID. 1001 advisory committee's note. Article X of the Federal Rules of Evidence codified the common law best evidence rule, terming it instead the 'original writing rule.'" *Id.*

¹¹ See, e.g., Craig Ball, "Don't Mess With System Metadata" Law Technology News, April 23, 2009, available at <http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202430116124>.

¹² See, e.g., *Krumwiede v. Brighton Assocs., L.L.C.*, 2006 WL 1308629 (N.D. Ill. May 8, 2006) (a plaintiff who destroyed metadata in the process of copying files was subject to a default judgment on the first four claims and ordered to pay costs—including expert fees and attorney fees—associated with the sanctions motion).

¹³ *In re Hawaiian Airlines, Inc., Debtor; Hawaiian Airlines, Inc. v. Mesa Air Group, Inc.*, 2007 WL 3172642 (Bkrtcy. D. Hawaii, Oct. 30, 2007) (company sanctioned when its Chief Financial Officer wiped files from his laptop computers after he was informed of a litigation hold notice).

¹⁴ All operating systems utilize mass storage devices (such as hard disks or flash drives) that are formatted with a file system. File systems typically have a system of allocating privileges for reading, modifying or otherwise utilizing files contained within the file system. For example, normal users are typically not allowed to modify files associated with the core software applications required for standard operation of the machine.

¹⁵ Typical operating systems include the various flavors of Microsoft Windows, Apple's OS X, and Linux.

¹⁶ One such tool is Ophcrack (<http://ophcrack.sourceforge.net/>), which is a Linux LiveCD that can be used to find the passwords associated with the Windows machine, including the administrator's password. Ophcrack is free and works on any flavor of Windows, including Vista. Another popular tool is "ntpasswd" which is freely available at: <http://home.eunet.no/pnordahl/ntpasswd/>. Ntpasswd can reset the administrator's password to whatever the employee desires. Note, the tools mentioned previously are commonly used by system administrators to fix problems encountered during the normal operation of PCs. These tools are not aberrant or illegal hacker software.

¹⁷ *Kvitka, supra*, n. 5, is a case where the plaintiff destroyed her laptop after being apprised that she was under an obligation to preserve it, and did not reveal the loss of the laptop to the Court when a judge asked her about the state of some of the contents of the laptop.

¹⁸ "The Sedona Conference on Legal Holds: The Trigger & The Process" (August 2007 Public Comment Version) by the Sedona Working Group at 12, citing *Zubulake V*. The paper is available at http://www.thesedonaconference.org/dltForm?did=Legal_holds.pdf

¹⁹ "Mesa could have taken reasonable steps that would have prevented, or mitigated the consequences of Mr. Murnane's destruction of evidence. For example, Mesa could have made a backup of Mr. Murnane's H drive and the hard drives of Laptop 1 and Laptop 2 promptly after HA filed suit. Doing so would not have been costly, burdensome, or unduly disruptive of Mesa's business. Instead, Mesa simply told Mr. Murnane to preserve all evidence and trusted him to comply. Even though Mr. Murnane was a valued, trusted, high level employee of the company, Mesa could and should have taken reasonable steps to prevent all of its employees from doing wrongful and foolish things, like destroying evidence, under the pressure of litigation. Because Mesa failed to take such steps, Mesa facilitated Mr. Murnane's misconduct." *In re Hawaiian Airlines, Inc., Debtor; Hawaiian Airlines, Inc. v. Mesa Air Group, Inc.*, 2007 WL 3172642 at *6 (Bkrtcy. D. Hawaii, Oct. 30, 2007).

²⁰ The Sedona Conference, "Commentary on Achieving Quality in the E-Discovery Process" (May 2009 Public Comment Version) available at: http://www.thesedonaconference.org/content/miscFiles/publications_html?grp=wgs110

²¹ See, e.g., *Wingnut Films v. Katja Motino Pictures Corp.*, 2007 WL 2758571, at *5 (C.D. Cal. Sept. 18, 2007) (a producing party must make a "reasonably diligent search for e-mails and other electronic documents").

²² "(a) Scope. Any party may serve on any other party a request (1) to produce and permit the party making the request, or someone acting on the requestor's behalf, to inspect, copy, test, or sample any designated 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, translated, if necessary, by the respondent into reasonably usable form, or to inspect, copy, test, or sample any designated tangible things which constitute or contain matters within the scope of Rule 26(b) and which are in the possession, custody or control of the party upon whom the request is served; or (2) to permit entry upon designated land or other property in the possession or control of the party upon whom the request is served for the purpose of inspection and measuring, surveying, photographing, testing, or sampling the property or any designated object or operation thereon, within the scope of Rule 26(b)." FRCP 34(a).

²³ See, e.g., *White v. Graceland Coll. Ctr. for Prof'l Dev. & Lifelong Learning, Inc.*, 2009 WL 722056 (D. Kan. Mar. 18, 2009) (although intrusive, "request for inspection for forensic or mirror imaging of computers [are] neither routine nor extraordinary.") citing *G.D. v. Monarch Plastic Surgery, P.A.*, 239 F.R.D. 641 (D.Kan. 2007); *Balboa Threadworks, Inc. v. Stucky*, No. 05-1157-JTM-DWB, 2006 WL 763668 (D.Kan. Mar. 24, 2006); *Jacobson v. Starbucks Coffee Co.*, No. 05-1338-JTM, 2006 WL 3146349 (D.Kan. Oct. 31, 2006).

²⁴ See, e.g., *Kipperman v. Onex Corp.*, 2009 WL 1473708 (N.D. Ga. May 27, 2009) (court imposed \$1,022,700 sanction for discovery abuse); *Oz Optics, Ltd. v. Hakimoglu*, 2009 WL 1017042 (Cal. App. Apr. 15, 2009) (appellate court upholds \$90,000 sanction); *Bray & Gillespie Mgmt. LLC v. Lexington Ins. Co.*, 2009 WL 546429 (M.D. Fla. Mar. 4, 2009) (court imposed sanctions on plaintiff and counsel).

²⁵ Hard disks do fail, more often after a few years of non-use, which is well within the time period of lawsuits. Many vendors who store data know this, and offer to "spin up" the hard disk periodically to ensure operation over extended periods of time.

This paper provides legal and factual information, as well as opinions from experts qualified by U.S. Courts. However, such information is not the same as legal advice and should not be construed as such. Please consult a lawyer if you want professional assurance that this information, and your interpretation of it, is appropriate for your situation.