

Summer, 2010

## THE CARBON FOOTPRINT OF E-DISCOVERY

by: Michelle A. Menely, Esq. and Lydia A. Zakhari, Esq.  
Gordon Tomas Honeywell, Seattle

*[Ref: Pleadings and Practice, Para. 8.07]*

In the era of electronically discoverable evidence, those involved in the litigation process – lawyers and insurance professionals, as well as their clients and insureds – must reconsider how they communicate. The issues evolving in e-discovery are particularly relevant to insurance professionals who in the claims process communicate with many parties, including insureds, claimants, witnesses, and counsel. The insurance professional also communicates internally with others in the company. Reports, e-mails, and drafts of letters created with a word processing program are but a few of the documents we all now trust to our computers or smart phones. As we will discuss, insurance professionals and lawyers have to conduct their business knowing that what they record electronically may resurface in litigation disputes and that more than what was requested in discovery might end up with opposing counsel.

### DIGITAL DNA – METADATA

E-discovery cannot be discussed without the term “metadata” being used in the conversation. In fact, many pitfalls in litigation have come about because parties fail to recognize the extreme impact of metadata in the discovery process, and the care that is needed to ensure that the distribution of information in electronic format is protected. If you are scratching your head about the meaning of “metadata” and its impact in the business sector, consider the following explanation from the court in *Williams v. Sprint/United Management Co.*, 230 FRD 640 (D. Kan. 2005).

Metadata, commonly described as “data about data,” is defined as “information describing the history, tracking, or management of an electronic document.” Appendix F to *The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age* defines metadata as “information about a particular data set which describes how, when and by whom it was collected, created, accessed, or modified and how it is formatted (including data demographics such as size, location, storage requirements and media information).” Technical Appendix E to the *Sedona Guidelines* provides an extended description of metadata. It further defines metadata to include “all of the contextual, processing, and use information needed to identify and certify the scope, authenticity, and integrity of active or archival electronic information or records.” Some examples of metadata for electronic documents include: a file’s name, a file’s location (e.g., directory structure or pathname), file format or file type, file size, file dates (e.g., creation date, date of last data modification, date of last data access, and date of last

metadata modification), and file permissions (e.g., who can read the data, who can write to it, who can run it). Some metadata, such as file dates and sizes, can easily be seen by users; other metadata can be hidden or embedded and unavailable to computer users who are not technically adept.

The question you may be asking yourself is, “who cares?” Well, the answer is that you should care because by providing electronic documents to an opposing party you may have provided your adversary with more information than you intended.

For example, presume your counsel is in the process of preparing a settlement letter. Your counsel has forwarded the document to you for review and comment. The document, as forwarded by your counsel, contains three paragraphs of text. After your review of the document, you determine that the third paragraph is unnecessary, or even unwise, and you insert the following comment with respect to that paragraph:

“I believe this paragraph should be deleted because I think it opens us, ABC Insurance Company, up to a never-ending obligation, and we never agreed to that in our settlement negotiations. Your thoughts?”

You then send the document to your counsel, and after discussion, the third paragraph including your comment is deleted. The document is then forwarded electronically to opposing counsel. Unfortunately, you and your counsel are unaware that opposing counsel has a hexadecimal data viewer application (hex editor) that allows him to view the deleted information (as well as other information) in the document. Opposing counsel uses that viewer and learns that you and your counsel had concerns (and what those concerns were) regarding the original third paragraph and that it was ultimately deleted. Counsel, being an obstreperous sort, now desires that the third paragraph be contained in the agreement or the settlement may fall apart.

As you can appreciate from this example, parties that routinely produce electronic documents in “native format” (i.e., the format in which it was originally created) can inadvertently produce unintended information to the opposing party. So, if a document request requires production in native format of all drafts of a contract and the contract has previously been transferred back and forth between client and counsel, each of the revisions, including any questions or comments imbedded in the document, will be available for viewing through a metadata viewer.

The Federal Rules of Civil Procedure specifically address production of electronic documents. *In re Classicstar Mare Lease Litigation*, 72 Fed. R. Serv. 3rd 922 (Callaghan) (E.D. Ky. 2009), involved a discovery request that resulted in production of 273,000 pages of documents by one defendant to all parties (the list of parties and their counsel fills almost 7 pages of the court’s decision). The court order resulting in production of these documents did not specify the format for electronic production, but the files were produced in a format compatible with litigation software used by all of the parties. A request was then made by one of the parties to have the documents produced in native format and the defendant objected. The court cited the applicable federal rule as Fed.R.Civ.P. 34(b)(2)(E)(ii) and said that under the rule, if the requesting party fails to specify a format in which it requests the information or documents, “a party must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms.” According to the court, an important consideration is whether the provided format “significantly degrades” the electronic searchability of the documents. In *Classicstar Mare*, the party that sought the discovery in native format produced correspondence with the defendant that established that even though it would cost \$15,000 for software to search the documents in native format, the party was willing to make that expenditure and had expected the discovery to be in native format. It was pointed out to the court that with the documents in the format as received it would be necessary “to manually sort through tens of millions of rows of densely formatted financial data.”

Rather than rely solely on the wording of the request under the civil rules, the court believed that the parties had previously reached an understanding that the documents would be produced in native format and that the defendant understood that without the documents in this format, the data would be considered degraded. A small victory for the defendant was that since the original document request did not specify native format and the defendant had already provided the requested documents, the court ordered the plaintiff to pay for the cost of providing the data in native format. The lesson is that in the absence of a specific request for native format (or, as in this case, extenuating circumstances) documents can be produced in hard copy or electronically without embedded metadata if they are considered “reasonably usable” forms.

If data must be produced in native format, a “scrubber” can be used (if permitted by the court) prior to providing the documents. A scrubber is a software program that filters and strips metadata from documents. While a scrubber program will not solve all metadata concerns, a number of issues can be avoided, including those in the example of the correspondence between the adjuster and counsel discussed earlier.

This is a mere introduction to metadata and compliance under the federal rules. Many issues remain with respect to production of documents in native format, including waiver of attorney-client privilege, whether a party receiving inadvertent production of electronic documents containing metadata can use the data or is obligated to return the documents to the producing party, and whether scrubbing is permissible in all cases.

## **SANCTIONS RELATED TO E-DISCOVERY**

According to Black’s Law Dictionary, spoliation of evidence is “the intentional destruction, mutilation, alteration, or concealment of evidence.” Sanctions for spoliation have been part of American jurisprudence for nearly a century. This jurisprudence was adopted in the context of “electronic discovery” in 2003 when Federal District Court Judge Shira A. Scheindlin (S.D.N.Y.) issued a series of opinions addressing the issue of whether, and to what extent, spoliation sanctions should be imposed for a litigant’s failure to preserve, maintain, locate, and produce electronically stored documents. In May 2010 Judge Scheindlin issued another opinion addressing that same subject in *Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities, LLC*, 685 F. Supp. 2d 456 (S.D.N.Y. 2010). Judge Scheindlin specifically stated:

By now, it should be abundantly clear that the duty to preserve means what it says and that a failure to preserve records – paper or electronic – and to search in the right places for those records, will inevitably result in the spoliation of evidence.

Judge Scheindlin addressed the various levels of “misconduct” that can give rise to a finding that spoliation sanctions should be imposed, and determined that the failure to engage in conduct aimed at maintaining and preserving electronic evidence can be considered “gross negligence” and can subject a party to sanctions when a party fails:

to issue a written litigation hold; to identify all of the key players and ensure that their electronic and paper records are preserved; to cease the deletion of email or to preserve the records of former employees that are in a party’s possession, custody or control; and to preserve backup tapes when they are the sole source of relevant information or when they relate to key players, if the relevant information maintained by those players is not obtainable from readily accessible sources.

Judge Scheindlin additionally stated that parties to a litigation:

need to anticipate and undertake document preservation with the most serious and

thorough care, if for no other reason than to avoid the detour of sanctions.

Judge Scheindlin also explained that if a party has spoliated evidence by failing to produce or preserve electronic evidence, determining whether sanctions should be imposed, and what level of sanction, requires a multi-step process.

- ◆ The first is the litigant's level of culpability – that is, was their conduct of discovery acceptable or was it negligent, grossly negligent, or willful.
- ◆ The second is the interplay between the duty to preserve evidence and the spoliation of evidence.
- ◆ The third is which party should bear the burden of proving that evidence has been lost or destroyed and the consequences resulting from that loss.
- ◆ The fourth is the appropriate remedy for the harm caused by spoliation.

Of course, the level of sanction depends on the level of culpable conduct, with the least culpable conduct giving rise to the least severe sanction. The sanctions that can be imposed include cost-shifting; fines; special jury instructions pertaining to inferences that may, or can, be drawn from the destruction of the evidence; and for sufficiently egregious conduct (e.g., the intentional destroying of evidence by burning, shredding, or wiping out computer hard drives), terminating sanctions (those that end the offending party's participation in a case, usually dismissal or default).

Thus, the question becomes how do you and your insureds avoid engaging in conduct that could result in sanctions?

Insurers, their insureds, as well as involved attorneys, must be cautious and heed the guidance given by Judge Scheindlin. That is, when an insurer receives notification of a claim against it, or against its insured, steps must be taken to preserve electronic evidence. Indeed, the claims professional and insured must keep in mind, from the time of the initial communication with an insured or third party, that discovery relating to electronic records will very likely be forthcoming and, thus, steps must be taken to ensure that discovery can be produced in a "readily accessible" form.

The issue of an insurer's duty to preserve evidence in a readily accessible format was addressed in *Continental Cas. Co. v. St. Paul Surplus Lines Ins. Co.*, 265 FRD 510 (E.D. Ca. 2010). The underlying case involved a claim for wrongful death. The decedent was killed while operating a forklift that was manufactured and maintained by Crown Equipment Corporation and that was leased by Tasq Technology, Inc. Both Tasq and Crown tendered defense of the wrongful death action to Continental. Continental accepted Tasq's tender (but initially denied Crown's) and immediately appointed defense counsel. Approximately two years later, Continental assumed Crown's defense in the underlying action subject to a reservation of rights.

During its defense of the underlying action, and just shortly before a scheduled settlement conference, Continental issued two letters to Crown's primary liability insurer, St. Paul. The letters advised St. Paul of the settlement conference and invited St. Paul's participation. Despite having been aware of the underlying action since the time it was originally filed, however, St. Paul did not respond to either communication. Continental then paid the underlying settlement and brought a contribution action against St. Paul.

Multiple discovery disputes arose between St. Paul and Continental. One issue was whether spoliation sanctions should be imposed against St. Paul based on St. Paul's "failure to create, maintain and preserve litigation or claim files relative to the wrongful death action." In bringing its motion, Continental asserted that St. Paul should have created such a claim file and "maintained all

relevant documents therein” from either the time of the original notification that the underlying action had been filed (June 2002) or, by the latest, at the time Continental invited St. Paul’s participation in the settlement of the underlying case (October 2006). Continental urged that St. Paul should be sanctioned because the “failure to maintain this evidence demonstrates a deliberate effort to avoid retaining materials” that may have been adverse to St. Paul. St. Paul’s argument was that “it was not required to open any file in the wrongful death action unless and until Crown tendered its defense by paying the \$250,000 SIR.”

In addressing the motion for sanctions, the California district court first noted that:

the duty to preserve relevant evidence can arise even before the commencement of litigation, and sanctions may be imposed if Defendants knew or should have known that the evidence destroyed was potentially relevant. ... The destruction of evidence need not occur after the specific evidence at issue was requested; rather sanctions may be imposed against a litigant who is on notice that documents and information in its possession are relevant to litigation, or potential litigation, or are reasonably calculated to lead to the discovery of admissible evidence, and destroys such documents and information.

The district court then turned to the issue of whether St. Paul “should have” opened a litigation file as contended by Continental. The court said:

the obligation of an insurer to open a litigation or claim file is necessarily triggered, respectively, by a reasonable assessment that potential litigation is likely or by an insured’s tender of a claim.

St. Paul argued that the triggering event had not occurred since Crown had not tendered, and because “it did not anticipate litigation because it was the practice of Crown to handle its own defense against potential liability within the SIR limits.”

The court ruled in St. Paul’s favor. The court did so, however, because it could not find “California authority clarifying when an insurer becomes obligated to open a file.” Despite ruling in St. Paul’s favor the court demonstrated extreme skepticism stating:

The argument that an insurer could reasonably conclude it may have little or no liability in a wrongful death action alleging defects in the machinery it insures is, to say the least, problematic.

The court next addressed whether St. Paul’s actual destruction of documents should give rise to a spoliation sanction. Continental argued that it had been prejudiced because letters it had sent to St. Paul should have been produced in discovery and were not. St. Paul admitted that the relevant letters had been destroyed but asserted that Continental could not show any prejudice because Continental itself authored the letters and, thus, presumably knew what information was contained in the letters. In response, Continental asserted that the letters had evidentiary value because the letters would likely have internal markings, marginalia (notes in the margins), and the like, which would tend to demonstrate what St. Paul knew, when St. Paul knew it, and what St. Paul’s initial reaction and response to the letters had been.

The court imposed a spoliation sanction against St. Paul. In doing so, the court stated:

The court finds St. Paul’s destruction of Continental’s letters is inexplicable and inconsistent with its obligation to maintain documents relevant to a potential litigation.

Despite finding that spoliation sanctions were appropriate the court imposed a modestly severe sanction – an adverse inference (a detrimental conclusion presumed from a party’s failure to produce evidence within its control). The court did so, primarily, because Continental did not suffer prejudice since it indeed had the documents in question (albeit without the marginalia). Thus the court determined that neither “dismissal of a claim or defense, nor the exclusion of witness testimony is warranted by this limited destruction of evidence.”

The court’s relatively minor sanction, an adverse inference, was remarkable considering that St. Paul apparently admitted it had destroyed documents. The California district court, however, is not alone in imposing only an “adverse inference” in the context of possible intentional destruction of documents. Indeed, courts in other cases have held likewise. See, e.g., *Rimkus Consulting Group, Inc. v. Cammarata*, 688 F. Supp. 2d 598 (S.D. Tex. 2010) (despite allegations of intentional destruction of documents, determining whether sanctions should be imposed, and level of sanction, required court to consider both spoliating party’s culpability and the level of prejudice to the opposing party); *In re Napster, Inc.*, 462 F. Supp. 2d 1060 (N.D. Cal. 2006) (adverse inference instruction warranted when destroying party had “culpable state of mind” and “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). Courts generally find sufficient culpability when the party had notice that documents were potentially relevant to the litigation before they were destroyed.

### **WHOSE JOB IS IT ANYWAY?**

The next question is whose obligation is it to make certain that an insured has received proper instruction and guidance on “preserving electronic evidence.” This issue was addressed in *In re A&M Florida Properties II, LLC*, 2010 WL 1418861 (Bankr., S.D.N.Y., April 7, 2010). In that case the court found that it is the attorney’s obligation to ensure that a client fully understands and complies with obligations in producing electronically stored documents and that the attorney’s failure to ensure client understanding will result in sanctions – against the client and the attorney.

The *Florida Properties* case involved a claim for breach of a \$41 million Purchase and Sale Agreement. During discovery, defendant American Federated Title Corp. issued discovery requests aimed at retrieving, among other things, copies of e-mail communications – e-mail communications that defendant knew existed. When the documents were not produced, discovery disputes arose. Information obtained during the discovery dispute revealed that the documents were not produced because proper searches had not been undertaken. The proper searches were not undertaken because counsel for GFI (one of the plaintiffs) failed to familiarize himself with the “detailed workings” of the client’s computer files and, thus, did not know how to adequately direct his client to produce the relevant documents. That is, the attorney did not know that the client’s e-mail records were contained in both “live” and “archive” folders. Thus, when counsel issued a directive to perform a “company-wide” search, the search did not include archive folders and documents contained in those files were not produced. The error was compounded when a forensic technician was hired, but the technician was not advised of the live versus archive e-mail folders either. While the forensic expert’s search revealed additional documents, it did not reveal documents that were contained in archive folders. After being informed that documents defendant knew existed had not been produced, the forensic expert opined that the “only possible explanation for the message’s absence was that someone at GFI deleted it.” In response to the assertion that documents had been intentionally deleted, counsel for GFI made further inquiry and learned of the archive folders. The forensic expert returned to GFI, located all responsive documents and those documents were eventually produced to American Federated.

Despite eventually obtaining the documents, American Federated moved for sanctions against GFI and its counsel, “for intentionally obstructing the discovery process.” Because the documents were eventually produced, the trial court declined to impose terminating sanctions, but the court did

impose monetary sanctions and, in doing so, severely admonished GFI's counsel, stating:

While the delays in discovery were not caused by any intentional behavior, GFI's counsel did not fulfill its obligation to find all sources of relevant documents in a timely manner. Counsel has an obligation to not just request documents of his client, but to search for sources of information. Counsel must communicate with the client, identify all sources of relevant information, and 'become fully familiar with the client's document retention policies, as well as the client's data retention architecture.' Counsel failed in his obligation to locate and produce all relevant documents in a timely manner. A diligent effort would have involved some sort of dialogue with ... key figures at GFI to gain a better understanding of GFI's computer system.

The lesson of the *A&M Florida Properties II, LLC* case is do not rely on your insured to know how to respond to discovery without guidance, especially since in that case the original search was conducted by the insured's chief technology officer. Instead, this task must be undertaken with guidance by counsel, or a forensic expert. While additional fees may be incurred by counsel in obtaining information about the client's business practices, the fees may well be worth it in the long run.

### **THE COOPERATION CLAUSE**

The failure to preserve, maintain, and produce electronic discovery can affect the litigation process and defense strategy.

- ◆ First, as discussed earlier, the failure to do so can subject parties to discovery sanctions.
- ◆ Second, the cost of producing electronic discovery can be significant and thus, can often drive the parties to settlement negotiations simply to avoid the expense of producing electronic documents.
- ◆ Third, a client's failure to maintain, preserve, and produce electronic discovery may have coverage implications because failing to produce can be a breach of the cooperation clause.

Most, if not all, insurance policies include a cooperation clause. A breach of the cooperation clause will relieve the insurer of liability if the failure to cooperate is substantial and the insurer has suffered prejudice as a result of the breach. In the context of a defense case, one way prejudice can be shown is to prove the insured neglected to disclose information needed by the insurer to prepare a defense. In the context of a coverage case, an insurer can demonstrate prejudice if the insured failed to produce documents or information that prejudiced the insurer's ability to determine coverage.

Since e-discovery is relatively new, cases specifically addressing the cooperation clause in the context of production of e-discovery (or failure to produce) are scarce. While the exact scenario of whether failing to produce electronic files and information is a breach of the cooperation clause may have not yet been addressed in the courts, how courts have treated the failure to produce physical documents can be instructive. That issue was addressed in *Martinez v. Infinity Ins. Co.*, 2010 WL 2169601 (C.D. Cal. May 20, 2010). The plaintiff in *Martinez* submitted a claim for theft of her automobile. The insurer suspected fraud and during its investigation of the claim, sought production of, among other things, financial documents, car payment records, and maintenance records. The insured delayed for months in providing some of the documents and completely failed to provide other requested information.

In holding the insured's failure to cooperate relieved the insurer of its obligations, the court noted

that the failure to produce records, in and of itself, can prejudice the insurer as a matter of law because without access to the requested documents the insurer cannot evaluate the validity of the claim.

There should be no real dispute that the rule that failure to produce hard copy financial information and records is a breach of the cooperation clause will also apply to failure of an insured to produce electronic records. Instead, the critical question is whether an insured's failure to take adequate steps to preserve and maintain electronic files so the information can be produced when, or if, litigation arises is a breach. As in other e-discovery cases, this determination will very likely depend on the extent of the insured's culpable conduct. That is, if the insured undertook to purposefully destroy evidence to avoid producing the information to an opposing party, and the insured thereafter suffers a terminating sanction, the insurer would certainly be able to assert that the insured failed to assist in the defense of the case and that it was subsequently prejudiced, and should therefore be relieved of its obligation to indemnify an insured for the loss. If the insured, however, merely negligently destroyed electronic evidence, the contrary may be true. Again, an insurer must prove actual prejudice to invoke breach of the cooperation clause as basis for denying coverage.

## CONCLUSION

This article may have caused you some pause, or even caused you to question your internal document management practices. Perhaps, you have come to question the information that may be discoverable in the e-mail you just sent to your attorney. Take comfort in knowing that everyone, including justices of the Supreme Court of the United States, is struggling to deal with the frontier of technological advancement. During oral arguments in the case of *City of Ontario v. Quon*, 130 S. Ct. 2619 (2010), Chief Justice John G. Roberts, Jr. asked: "maybe everybody else knows this, but what is the difference between the pager and the e-mail?"

It is important for you and your counsel to take the steps necessary to protect your company and its insureds from discovery violations that could result in severe sanctions. Additionally, as the electronic landscape expands, you and your counsel should be mindful of the nontraditional avenues of investigation that can be beneficial in claims investigation and litigation.

In an era in which communication via electronic mail, text messaging, and social-networking has trumped what used to be face-to-face meetings and telephone calls, the way we interact with each other is now constantly being documented and archived.

Michelle A. Menely, MMenely@gth-law.com, and Lydia A. Zakhari, LZakhari@gth-law.com, are attorneys with the firm of Gordon Tomas Honeywell LLP, 600 University Street, Suite 2100, Seattle, Washington 98101 (206-676-7500), www.gth-law.com.

This article is an introduction to metadata and its impact on discovery, requirements for electronically storing and providing information, sanctions related to e-discovery, and how the insurance policy's cooperation clause applies to e-discovery. These topics and many other e-discovery issues will be presented in more detail by Ms. Menely in November at the 2010 SCLA Conference in San Antonio. www.sclasociety.org.