

Ungaretti & Harris LLP
E-Discovery Update

**E-Discovery in Practice:
Report from a Trial**

by Lisa C. Sullivan

E-discovery violations most often are uncovered during the discovery process. In other words, a witness mentions something at deposition, or a document's format or content suggest that other similar documents exist. Sometimes, though, evidence of e-discovery violations is revealed mid-trial. Of course, no party wants to be the one sitting in front of the judge and the jury admitting that electronic documents have not been searched, let alone produced. On the other side of the coin, the attorney who uncovers an e-discovery violation during trial needs to know the best way to respond and to use this to the client's advantage.

Ungaretti Uncovers E-Discovery Violations Mid-Trial

At cross-examination during a recent jury trial, Ungaretti & Harris discovered that the plaintiff had failed to produce an entire database of relevant documents. With several attorneys well-versed in e-discovery, Ungaretti was able to quickly and appropriately respond.

The Written Discovery Requests

The plaintiff sought damages in the form of lost profits for sales of goods. During discovery, Ungaretti had sought production of documents relevant to the claimed profits – such as documents about the plaintiff's manufacturing

costs. In response, the plaintiffs had represented that no such documents existed.

Admission That a Database Exists

At trial, the plaintiff's corporate representative testified, based on his experience, about some of the components of cost. On cross-examination, Ungaretti sought to verify whether it was true that the plaintiff maintained no documents about its manufacturing costs. On the stand, the witnesses admitted that while the company had no documents "per se," it did maintain information in a computerized database.

Cross-Examination

Of course, this led to immediate cross-examination about the database in front of the jury. The plaintiff's witness admitted that the database had information on raw material inventory – and that this was not provided to the defendant. The plaintiff's witness admitted that the database had information on incoming shipments of parts – and that this was not provided to the defendant. By the end of cross-examination, the jury understood that a whole wealth of information had been withheld from the defendant.

The e-discovery story did not end there. Counsel requested the opportunity to further question the plaintiff's witness outside the presence of the jury about this apparent serious e-discovery violation, and the judge permitted significant examination. Counsel asked whether the plaintiff had done anything whatsoever to search the electronic database to find answers to the defendant's discovery requests. The witness admitted that no one from the company had bothered to do so. Indeed, he asserted that the electronic data were "not documents." What's more, the witness admitted that he had gathered information from that same electronic database at the request of plaintiff's expert witness on damages. The distinction was, in his mind, that the expert had not requested "documents," he had requested "data."

The cardinal sin committed there is glaringly apparent to anyone familiar with e-discovery. Rule 34 of the Federal Rules of Civil Procedure makes no such distinction between "documents" and "data." To the contrary, Rule 34 includes within its scope "electronically stored information." The 2006 Advisory Committee Notes explain:

Electronically stored information may exist in dynamic databases and other forms far different from fixed expression on paper. Rule

Contents

E-Discovery in Practice: Report from a Trial
by Lisa C. Sullivan

Two Lessons on How and When to Retain Data
by Richard H. Tilghman IV

Illinois Court Rules That There May be No Automatic Right to Metadata Unless Specifically Requested
by Nile Park

Who Is Your Defendant?
Determining the Right Entity to Sue on the Internet
by Emily M. Dierberg

The Perils of Tweeting Angry: Facebook Postings and Similar Social Networks Posts are Discoverable
by James M. Carlson

34(a) is amended to confirm that discovery of electronically stored information stands on equal footing with discovery of paper documents. . . . [A] Rule 34 request for production of “documents” should be understood to encompass, and the response should include, electronically stored information unless discovery in the action has clearly distinguished between electronically stored information and “documents.”¹

As touched on many times in this newsletter, the changes to discovery rules regarding digitally stored documents are very important and a party can easily be trapped if not careful.

Motion for Sanctions

After this cross-examination, the court granted Ungaretti leave to file a written motion for sanctions during trial. This was done on an expedited basis by the firm. Ungaretti sought, as a sanction, dismissal of the plaintiff’s damage claim.

Result

In the end, the jury ruled in favor of Ungaretti’s client, and found that the appropriate amount of damages to be awarded was “\$0.” At press time, the motion for sanctions remains under consideration by the judge.

Conclusion

At this point in the history of e-discovery case law, companies are now familiar with the range of sanctions judges can impose for mismanaging production of electronic documents—from monetary sanctions to dismissal of claims or default judgment. What hasn’t gotten as much attention is the reaction of juries when they learn that a party has kept electronic data secret. In this jury trial, Ungaretti’s opponent learned that failure to abide by e-discovery obligations can be just as devastating – if, of course, the lawyers know how to respond quickly and comprehensively.

¹ Fed. R. Civ. P. 34, 2006 Advisory Comm. Notes.

evidence. Instead, the basis for the plaintiff’s allegation was that the plaintiff expected to find more documents than were produced.

In response, the defendant tried to explain the absence of data based on its data retention practices, noting that employees are responsible for archiving e-mails that are deemed necessary to perform the employees’ job functions. The court was unimpressed, holding that a responsible data management policy requires accountability to third parties and that allowing operations-level employees to control data retention is unreasonable.

Also of note, the court rejected the defendant’s position that its preservation duty did not arise until it was notified by the plaintiff of a potential lawsuit. Instead, the court held that the defendant was on notice of potential litigation approximately five years prior to plaintiff’s notice, based on activities occurring in the industry. Specifically, a variety of class action lawsuits had been filed arising out of the floppy disk errors addressed by plaintiff’s technology. In holding that the duty to preserve arose during this industry activity, the court analogized to cases holding that a party has a duty to preserve evidence from a fire even when it is unclear if the fire will result in litigation. Finding that the defendant had not met its preservation obligations, the court awarded sanctions, but withheld ruling on the amount of sanctions until the close of fact discovery.

Two important lessons emerge. First, organizations should not give operations-level employees control over data retention. Instead, organizations must have a formal policy created and implemented by supervisory personnel. Second, extraordinary developments in an organization’s industry can affect the organization’s duty to preserve evidence if those developments should put an organization on notice of potential litigation. If sufficiently significant, such developments can implicate a duty to preserve evidence before litigation begins, or even before the plaintiff gives notice of potential litigation.

¹ *Phillip M. Adams & Associates v. Dell, Inc.*, No. 1:05-CV-64 TS (D. Utah Mar. 27, 2009) (Judge Nuffer).

Two Lessons on How and When to Retain Data

by Richard H. Tilghman IV

A recent case, *Phillip M. Adams & Associates v. Dell, Inc.*¹, provides two important lessons for knowing how and when to retain electronic data. In *Phillip M. Adams*, the plaintiff alleged that the defendant had destroyed data demonstrating that the defendant was pirating the plaintiff’s proprietary technology for solving data corruption in floppy disks. Despite the plaintiff’s allegations of destruction, there was “no direct proof” that the defendant had destroyed

Illinois Court Rules That There May be No Automatic Right to Metadata Unless Specifically Requested

by Nile Park

In *Autotech Technologies Limited Partnership v. Automationdirect.com, Inc.*¹, the United States District Court for the Northern District of Illinois held that a party requesting production of electronically stored information must specifically request metadata and that absent a request for a specific form of production, a PDF satisfies

the “reasonably usable form” requirement under Federal Rules of Civil Procedure 34(b)(2)(E)(ii). This ruling is a considerable outlier from previous case law that seemed to indicate that a party’s right to review metadata was as inherent as the right to request copies of relevant hardcopy documents.

As readers of this newsletter know, metadata can be a fruitful source of valuable information. In fact, metadata can indicate the date that a document was created, when it was modified, when it was last printed, and who last edited it. More importantly, metadata can show recent edits to the content of a document. In *Autotech*, the requesting party was dissatisfied with the production of PDF files in response to discovery requests. Such PDF files do not include the type of metadata that would be most useful during the discovery process. Here, the requesting party in *Autotech* moved to compel production of Microsoft Word files of the PDF formatted documents.

At issue in *Autotech* was whether a PDF file of the document that did not have the desired metadata is “in a reasonably usable form” under Federal Rules of Civil Procedure 34(b)(2)(E)(ii), which states: “[I]f a request does not specify a form for producing electronically stored information, a party must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms.”

In this case, the requesting party did not specify the desired form of the document or request metadata. In fact, the requester only thought of metadata for the first time after paper copies were produced. In retrospect, this was a turning point in the discovery process for this case. Parties must be aware that metadata should almost always be asked for at the discovery phase if not at the initial meeting between the parties that is required by Federal Rule of Civil Procedure 26.

In reviewing the motion to compel, the Court clearly focused on the fact that the request for metadata was relatively new. The Court claimed that it was “a little late” to ask for metadata after responsive documents have been produced, stating, “[O]rdinarily, courts will not compel the production of metadata when a party did not make that a part of its request.”

In this case, the Court concluded that unless a requesting party specifically asks for metadata or unless metadata is relevant to the claims and defenses of the litigation and the court orders production of metadata, producing a PDF file satisfies the “reasonably usable form” requirement. The Court noted in its opinion that “[T]here should be a modest legal presumption in most cases that the producing party need not take special efforts to preserve or produce metadata.” The Court denied the defendant’s request for production of the native file format (here Microsoft Word version) of the documents at issue.

This case instructs parties to take an aggressive approach to electronic discovery, as there is no automatic right to metadata of electronic documents unless it is specifically requested. It serves as a clear warning to parties seeking such metadata – remain silent at your own risk.

¹ 248 F.R.D. 556 (N.D. Ill. Apr. 2, 2008).

Who Is Your Defendant? Determining the Right Entity to Sue on the Internet

by Emily M. Dierberg

Is someone selling a product that is substantially similar to your company’s product over the Internet? Is someone offering a bootlegged version of your media, or pirating your software? Are they using your trade name or copying your information and holding it out as their own? Even worse, did they illegally obtain your company’s actual products and are offering to sell those products at a discount?

All of the above-mentioned activities constitute violations of the law. To stop this from happening, you will likely begin by sending a “cease and desist” letter demanding that the perpetrator or infringer refrain from engaging in the unlawful activity. If the unwanted activity continues, it may be the right time to pursue litigation.

However, you cannot initiate litigation against a defendant, or even directly communicate with an infringing individual, if you don’t know who you are actually pursuing. Unfortunately, the Internet does not always identify the correct party to deal with in such circumstances. Today’s highly technological society and the use of the Internet present new obstacles in locating the individuals or groups behind unlawful Internet activity. Potential defendants may attempt to hide behind a webpage to conceal their identity to avoid being sued.

With fairly simple methods, however, you can find the true individual behind any domain name. WHOIS is the Internet function that allows anyone to investigate domain registration information. By performing a WHOIS search, you can discover when and by whom a domain was registered, contact information, and more. A WHOIS search can also reveal the name or network mapped to a numerical IP address.

To engage in this process, simply find out the domain name of the website conducting the unlawful activity. Then, go to whois.com, enter the domain name in the lookup box, and the lookup will locate the person to whom the domain name is registered. With this information, you or your company at least have a beginning place to start when considering action against the host of the website.

It is important to realize that some of the information on WHOIS is potentially outdated or even more cryptic than a blank web page. However, these first steps of indentifying the proper individual to sue can be very useful to a plaintiff considering an action against a web-based defendant.

**The Perils of Tweeting Angry:
Facebook Postings and Similar Social
Networks Posts are Discoverable**

by James M. Carlson

While web-based social networking sites like Facebook, MySpace, and Meetup.com have become very popular, they also pose potential problems for parties engaged in litigation. Recent case law indicates that the information stored on such Internet sites is not only discoverable but that there is little to no expectation of privacy for individuals seeking to protect such information. This is a double-edged sword for companies involved in litigation.

Companies certainly need to make sure that their own employees do not have damaging information stored on these sites. This could range from discussing privileged business information or cataloging potentially harassing behavior. However, such sites may also prove to be a treasure chest of discovery under the right circumstance. Many individuals put all kinds of information on social networking sites. This is a dangerous practice. Although, it can be very fruitful if the individuals are on the other side of the courtroom. But make no mistake – this information is discoverable and the right attorneys can locate and exploit it.

In *Ledbetter v. Wal-Mart*¹, a United States District Court allowed Wal-Mart to subpoena the information kept on various social networking sites regarding the personal

habits and activities of the plaintiffs. In this case, the plaintiffs are electricians who were allegedly injured while working at a Colorado Wal-Mart store. The plaintiffs sued Wal-Mart claiming that their injuries had, among other things, seriously affected their lifestyles. One of the plaintiffs' wives also claimed loss of consortium because of the injuries.

During the discovery process, Wal-Mart's attorneys found that the plaintiffs, and their significant others, had posted information on certain social networking sites (Facebook, MySpace, and Meetup.com) that were relevant to the claims at issue. For example, one of the plaintiffs had claimed that he was so severely injured that he was unable to go out in the sun and was unable to enjoy his favorite fishing hobby. Wal-Mart's attorneys, however, found alleged examples of the plaintiff sunning himself outside and enjoying fish trips after the date of his accident. Wal-Mart's attorneys sought to review all of the information submitted to these sites.

Wal-Mart's attorneys issued subpoenas to these social networking websites. In order to protect this information, the plaintiffs filed a motion for protective order that would have prevented the websites from disclosing the information. In the motion, the plaintiffs claimed that the information should be protected by, among other things, the physician-patient privilege or the spousal privilege. The court denied the motion for protective order and allowed Wal-Mart to issue the subpoenas.

Currently, the websites involved in this lawsuit have yet to produce the information sought by Wal-Mart. The plaintiffs claim that they no longer control the information and that it is in the control of the websites. This newsletter will continue to monitor the evolution of this case and others like it.

¹ 2009 WL 1067018 (D. Colo. April 21, 2009).

For further information on the E-Discovery and Document Management Group or this update, please contact one of our members:

- | | | |
|--------------------------|--------------|----------------------|
| James M. Carlson, Editor | 312.977.4143 | jcarlson@uhlaw.com |
| Tina B. Solis | 312.977.4482 | tbisolis@uhlaw.com |
| Lisa C. Sullivan | 312.977.4465 | lcsullivan@uhlaw.com |
| Jessica K. Thomas | 312.977.4498 | jkthomas@uhlaw.com |
| Emily M. Dierberg | 312.977.4122 | emdierberg@uhlaw.com |
| Steffany L. Hreno | 312.977.4347 | slhreno@uhlaw.com |
| Nile N. Park | 312.977.4125 | npark@uhlaw.com |
| Richard H. Tilghman IV | 312.977.4881 | rhtilghman@uhlaw.com |
| Heidi Goldwater | 312.977.9215 | hgoldwater@uhlaw.com |

This **E-Discovery Update** has been prepared by Ungaretti & Harris LLP solely for informational purposes and does not constitute legal advice. This information is not intended to create, and receipt of it does not constitute, an attorney-client relationship. Readers should not act upon this information without seeking professional counsel.

© Copyright 2009 UNGARETTI & HARRIS LLP
www.uhlaw.com