

Ungaretti & Harris LLP
E-Discovery Update

**Data Mapping Your Opposition:
True Practice Stories and Lessons**

by James M. Carlson

This newsletter has discussed the use of data maps as an effective – if not necessary – tool in cataloguing a company’s data prior to facing the discovery requirements of production in litigation. Data maps are essentially a complete list of all of a company’s systems, the type of documents on those systems, and how those systems and documents interact. Data maps allow a company to have a general idea about how its electronically stored information is maintained and stored. Typically, data maps allow for pre-litigation protection and organization. However, there are other uses for data maps.

When engaged in litigation, it sometimes makes sense to create a data map of the opposing party’s systems. Of course, prudent counsel will always demand the production of any pre-existing data maps from the opposing party during discovery. The problem is that many companies have yet to create a data map or an opposition may refuse to fully cooperate during discovery. This can be a blessing in disguise. In fact, many times it is more instructive for a

party to go through the steps of creating the opposition’s data map in order to unearth valuable information.

In my practice, I have created data maps of the opposition’s computer systems based upon other electronically stored information unearthed during discovery. As a result, I have located certain “missing pieces” of the e-discovery puzzle and identified additional sources of information that the opposition had insisted did not exist. There have been numerous cases I have been involved in where I was forced to actively create the opposition’s “data map.” The thrust of discovery revealed many of the systems in use by the other side as well as the type of documents that were on its systems. By sifting through this information and creating a data map of our own, I was able to discover the existence of additional computer systems. In essence, the data map indicated that another computer system should have been included in discovery materials. This was based upon the way the surrounding data and systems were set up. Once pushed on this fact, the opposing party caved and produced documents from this newly discovered computer system.

Thinking about the opposition’s data in this way can bear significant fruit. In doing so, it forces a party, its legal counsel, and its experts to explicitly think about the systems in use by the opposition. In short, it allowed me to more broadly probe and understand the opposition’s data systems.

The purpose of creating data maps of your opposing party’s systems is to delve deeper into what electronically stored information they are truly keeping. When done correctly, it can produce valuable discovery and very useful information about an opponent.

Contents

Data Mapping Your Opposition:
True Practice Stories and Lessons

by James M. Carlson

The Federal Court of Claims Holds That Documents Be
Produced in the Usual Course of Business
Not in the Usual Course of Storage

by Nile N. Park

U.S. Federal Court Finds Gross Negligence for Failing to
Institute a Litigation Hold After Being
Served with a Complaint

by Richard H. Tilghman IV

Illinois Court Denies Unfettered Search of Computer
Systems: Lessons from *Mintel v. Neerghen*

by James M. Carlson

Tech Corner – Don’t Forget to Dot Your “I”s

by Heidi Goldwater

**The Federal Court of Claims Holds That
Documents Be Produced in the Usual
Course of Business Not in the Usual
Course of Storage**

by Nile N. Park

The Federal Court of Claims has recently made clear that documents produced in litigation must be organized as they were maintained during the course of business. The Court was not swayed by arguments that the documents were maintained in an organized fashion in storage.

Nor was the Court swayed by arguments that a mass production – without any explanation as to how the documents were responsive to certain discovery requests – was proper. The ruling has clear implications for hard copy documents, but also has implication for electronically stored information.

In *Ak-Chin Indian Community v. United States*¹, an Indian tribe filed a lawsuit against the U.S. government and a discovery dispute ensued regarding the government's responses to the tribe's discovery request and interrogatories. In response to the discovery requests, the government made available for inspection documents at a Kansas federal record storage facility called the American Indian Records Repository ("AIRR"). The documents at AIRR were indexed by software called Box Index Search System ("BISS"). As for its response to the interrogatories, the government referred the Plaintiff generally to "potentially relevant boxes of records" at AIRR "as set forth in the BISS query results." Unsatisfied with the government's responses, the Plaintiff filed a motion to compel.

The Court granted the Plaintiff's motion upon its analysis of the applicable discovery rules requiring that "a party must produce documents as they are kept in the usual course of business or must organize and label them to correspond to the categories in the request." The Defendant argued that it should be able to produce requested documents in the same organization as they were stored at AIRR. The Plaintiff countered that such production was improper and the Defendant must instead organize and label the documents to correspond to the categories in the Plaintiff's request.

The Court agreed with the Plaintiff and ordered the government to organize and label the documents because the AIRR documents did not meet the "in the usual course of business" requirement. The Court noted that the filing system for documents stored at AIRR was different from the one that was used when the documents were actively maintained by the government agency. The documents were "substantially rearranged and co-mingled with" other documents before it was shipped to AIRR for storage, and "[o]nce the documents are disassembled from their filing system at the agency office and reorganized to comport with the filing system at the AIRR, they are no longer kept 'in the usual course of business.'" The Court also stated that stored documents "are not kept in the usual course of business within the meaning of [the rules]" unless it can be "show[n] that the way in which the documents are kept [in storage] has not changed from how they are kept in the usual course of business."

Finally, a party challenging a filing system must "allege[] that the producing party's filing system is 'so disorganized"

that the propounding party is unable meaningfully to review documents." The Plaintiff in this case made such an allegation and the Court agreed. The Plaintiff was kept from reviewing the document because BISS searches produced inconsistent results; indexing by boxes containing potentially responsive documents is a labor-intensive process; and indexing on BISS effectively resulted in a "document dump."

Lastly, the Defendant's interrogatory response failed to meet the rule's requirement to "specify[] the records that must be reviewed, in sufficient detail to enable the interrogating party to locate and identify them as readily as the responding party could." Merely referring the Plaintiff to boxes that could potentially contain responsive documents was insufficient to meet the rule's requirement that the records to be reviewed be specified.

The implications of this ruling are very clear. First, documents must be produced as they were used by a party in its usual course of business. Second, broad "document dumps" in response to discovery requests are improper. These lessons apply to both hard copy and digitally stored information.

¹ 85 Fed. Cl. 397 (Fed. Cl. 2009) analyzes Rules of the United States Court of Federal Claims 33 and 34, which mirror Federal Rules of Civil Procedure 33 and 34.

U.S. Federal Court Finds Gross Negligence for Failing to Institute a Litigation Hold After Being Served with a Complaint

by Richard H. Tilghman IV

This newsletter has consistently reminded its readers of the importance of instituting litigation holds. Litigation holds ensure that potentially relevant documents – both electronic and hardcopy – are preserved for discovery during litigation. Best practices dictate that litigation holds should be instituted upon reasonable anticipation of litigation. At the very least, a party should issue a litigation hold once the complaint is served. Now, courts are beginning to punish those parties who do not do so. In fact, the United States District Court for the Eastern District of New York recently sanctioned a defendant for failing to institute a litigation hold.

In *Acorn v. County of Nassau*¹, the Eastern District of New York sanctioned the defendant, Nassau County, for failing to issue a proper litigation hold, even though there was no evidence that relevant information had been destroyed. In *Acorn*, Nassau County claimed it instituted a verbal hold at the beginning of the case and a written hold 15 months

later when its motion to dismiss was denied. Despite the County's argument that it was appropriate to institute a hold after its motion to dismiss was denied, the Court found otherwise, holding that the County was grossly negligent in failing to institute a hold upon being served with the complaint.

The County's only saving grace was that the Plaintiff could not establish that helpful materials were actually destroyed. As a result, the Court limited the sanctions to the fees and costs incurred by the Plaintiff in bringing the sanctions motion. While the sanctions imposed in *Acorn* were modest, the lesson for litigants is clear: courts will impose a bright-line requirement that parties must institute a litigation hold once litigation is anticipated. Although the failure to timely institute a hold did not result in catastrophic sanctions in *Acorn*, fees and costs are a potentially painful sanction.

It is overwhelmingly clear that the County should have done more than just verbally instruct its employees to retain certain documents. Moreover, a case like *Acorn* sets the groundwork for much broader and stiffer sanctions in future cases. In short, the failure to implement a proper litigation hold in writing can have a significant impact where it can be shown that relevant information was destroyed. But as *Acorn* demonstrates, the failure itself – not whether or not documents were lost – may be sanctionable as well.

¹ *Acorn v. County of Nassau*, 2009 WL 605859 (E.D.N.Y. March 9, 2009)

Illinois Court Denies Unfettered Search of Computer Systems: Lessons from *Mintel v. Neerghen*

by James M. Carlson

In a recent case before the United States District Court for the Northern District of Illinois, the Court recognized that unfettered searches of computer systems will not automatically be granted – and the standard for obtaining forensic mirror images of third party computer systems may be quite high. This case is important because the judge outlined a number of issues faced by parties seeking broad discovery of electronically stored information. Two main lessons from this case are clear: (1) be prepared to narrow your requests for electronically stored information; and (2) when a court proposes a rational solution for recovering electronically stored information, be very careful about the option not to pursue it.

In *Mintel Inter'l Group Ltd v. Neerghen*¹, Mintel sued its former employee Neerghen. Mintel claimed that

Neerghen, while still working for Mintel, had e-mailed confidential documents to his personal e-mail account. Allegedly, Neerghen then took these documents to his new employer, Datamonitor, which is a competitor of Mintel's. Datamonitor is not currently a defendant in the proceedings.

Since the beginning of the litigation, Mintel has attempted to get a mirror image of Datamonitor's computer systems to obtain proof that Neerghen brought the Mintel documents to Datamonitor. Seeking such a broad forensic copy of a competitor's computer systems is admittedly a sweeping goal. This is especially true given that Datamonitor is not a party to the lawsuit. But Mintel argued that the documents allegedly held by Neerghen could have appeared on any of Datamonitor's systems.

The context of the requested discovery is extremely important. Prior to the most recent ruling, the Court offered that Mintel provide a list of search terms to Datamonitor's expert to conduct a search of Datamonitor's computers. Mintel did not pursue that option, and perhaps understandably. Mintel likely was concerned that Datamonitor's own expert would be favorable to Neerghen and would not be impartial. Mintel might have used this opportunity to push for a completely neutral expert to search Datamonitor's systems, but instead Mintel continued to push for a complete forensic copy of Datamonitor's systems.

The latest opinion in this case rules upon Mintel's motion to reconsider the Court's rejection of Mintel's latest request for a forensic mirror image of the Datamonitor computer systems. In bringing the motion to reconsider, Mintel presented newly discovered evidence. In particular, Mintel had examined USB drives produced by Neerghen that contained fragments of Mintel's documents. The USB drives only contained fragments because the contents of the USB drives had allegedly been wiped making full recovery impossible. Mintel's expert argued that the USB drives also indicated, however, that at least one of the Mintel documents had been printed on the Datamonitor systems to a Datamonitor printer server. Mintel's expert even discovered the exact name of the printer server. Mintel argued that this new evidence justified a forensic mirror image of Datamonitor's systems. In short, Mintel argued that there was enough smoke to imply a pretty significant fire.

The Court, however, disagreed. In denying the request for a complete mirror image of Datamonitor's systems, the Court made a number of crucial points. First, the Court noted that Mintel's analysis of the USB drives came after the deadline for expert reports. The Court viewed this lack of diligence in a poor light. Second, the Court

believed that unfettered access to a third party's computer systems requires a particularly strong showing. Here, the Court believed that it was more likely that the request for a complete mirror image of Datamonitor's computer systems was more speculative than grounded in evidence.

The result reached by the Court is significant and interesting. First, the Court struck a balance between the impulse for broad discovery and obtaining unfettered access to third party's computer systems. The Court felt that a party must make a fairly high evidentiary showing to proceed with such a broad swipe at discovery. In truth, that analysis may be an outlier when compared to many courts' broader views of electronic discovery. Second, the Court's ruling teaches litigants that a narrower, more focused approach to electronic discovery will more likely be embraced by a court. Wider ranging sweeps may be met with judicial resistance.

This newsletter will continue to monitor further developments in this case.

¹ *Mintel Int'l Group Ltd v. Neerghen*, Case No. 08 CV 3939 (N.D. Ill. February 3, 2009)

Tech Corner: Don't Forget to Dot Your "I"s

By Heidi Goldwater

Forensic acquisition of digital assets is becoming more of the norm in litigation, not the exception. If you are in the discovery phase of litigation and have been asked to collect ESI, it is crucial to remember that it exists everywhere. There are 3 areas of data collection that tends to slip by but should not be ignored. They are removable USB or jump drives, smart phones, and MP3 players.

These are the most important devices to remember because they are the ones most frequently used to covertly steal data from companies.

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	tbsolis@uhlaw.com
Kamau A. Coar	312.977.4343	kacoar@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

USB Drives

Everyone has them, as a matter of fact in the past 5 years jump drives have been a very popular promotional item. These devices are becoming cheaper everyday with increased storage capacity. People use them to backup files or to copy files for transport between a work and home personal computer. Unfortunately, they are also used to collect proprietary information. That is why it is critical that they are seized in litigation.

Former employees may think that they can covertly plug one of these drives into their corporate computer and copy files without detection. As described in the preceding article, that is not the case. Any good computer forensic examiner can identify the brand, size, serial number, and the last time a device was plugged into a computer. They may also be able to identify which files were copied to the drive.

Smart Phones

What exactly is a Smart Phone? Any device that is a telephone, e-mail device and/or a portable hand held personal computer. The most popular smart devices are the Blackberry and the iPhone. These devices no longer simply store e-mails. Many of them have programs which run GPS and other applications such as word-processing and spreadsheet applications. Additionally many of these devices have expansion slots for additional storage. So not only might there be data on the smart device, there could also be data stored on a memory card used in the device.

MP3 Players

There are many brands of MP3 players in the market place, such as the very popular iPod. While these devices play music, videos and games, they can also be plugged into a computer and used exactly like a USB drive for data storage. Additionally, the iPod Touch has the capabilities of a smart phone.

So, in the process of collecting ESI for litigation, it is crucial to locate all of the devices that are typically used to steal or conceal data.

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