

Ungaretti & Harris LLP
E-Discovery Update

7th Circuit Implements Pilot Program to Address E-Discovery Issues

By Richard H. Tilghman IV

Recognizing the burden and expense of producing electronically stored information in compliance with the Federal Rules of Civil Procedure, the 7th Circuit Court of Appeals Electronic Discovery Committee recently created a pilot program called the Principles Relating to the Discovery of Electronically Stored Information (Principles).¹ During the first phase of the pilot program, from October 2009 to May 2010, certain judges within the 7th Circuit have agreed to adopt the Principles in select cases through the entry of a standing order. After this trial period, the Principles will be assessed and refined by the 7th Circuit's Electronic Discovery Committee.

The Principles set forth a range of guidelines to assist parties in dealing with electronic discovery issues, with the goal of facilitating the just, speedy, and inexpensive resolution of civil cases through early resolution of electronic discovery disputes. Some of the highlights of the Principles include:

- An emphasis on the proportionality provision set forth in FED. R. CIV. P. 26(b)(2)(C)(iii), which allows the court to weigh the burden and expense of proposed discovery against its likely benefit, taking into account the "needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of discovery in resolving the issues." Principal 1.03.

- Encouraging counsel for each party to understand their client's data storage and retrieval systems before the Rule 26(f) conference. Principle 2.01(c).
- The appointment of "e-discovery liaison(s)" to assist the parties and the court in dealing with e-discovery issues. An e-discovery liaison must (1) be prepared to participate in e-discovery dispute resolution; (2) be knowledgeable about the party's e-discovery efforts; (3) be, or have access to those who are, familiar with the party's electronic systems; and (4) be, or have access to those who are, knowledgeable about technical aspects of e-discovery. Principle 2.02.
- Encouraging parties who make a preservation request to do so specifically and encouraging parties responding to a preservation request to provide specific, useful information to the requesting party. Principle 2.03.
- Specifying certain categories of electronically stored information that are "generally not discoverable in most cases" such as: (1) deleted, slack, fragmented, or unallocated data on hard drives; (2) random access memory or other ephemeral data; (3) on-line access data such as temporary internet files, history, cache, and cookies; (4) data in metadata fields that are frequently updated automatically; (5) backup data that is substantially duplicative of data that is more accessible elsewhere; and (6) "other forms of electronically stored information whose preservation requires extraordinary affirmative measures that are not utilized in the ordinary course of business." Principle 2.04(d)

Based upon the Principles (and in accordance with best practices for dealing with e-discovery issues), parties involved in litigation involving e-discovery should appoint an e-discovery point person to assist counsel with data preservation and retrieval issues and, potentially, to act as the "e-discovery liaison" in the event of an e-discovery dispute. The individual should be able to articulate the burden and expense of discovery requests based upon the party's information systems. Having a point person in place will allow for better coordination with outside counsel and provide an individual fully informed of the case's e-discovery issues if an e-discovery liaison becomes necessary.

While the efficacy of the Principles has yet to be determined, they provide the parties and their counsel with some guidance that, at least in theory, should assist in reducing the burden and expense of electronic discovery.

Contents

7th Circuit Implements Pilot Program to Address E-Discovery Issues

By Richard H. Tilghman IV

Format Specification Proves Crucial in *Cerveo* Case

By Emily M. Dierberg

E-Discovery Across International Borders

Part Two: U.S. Courts Tackle European Privacy Laws

By Lisa C. Sullivan

Tech Corner

Collecting Email Data for Litigation:
Knowing Where to Look

By Heidi Goldwater

¹ Available at: http://www.ca7.uscourts.gov/7thCircuit_Electronic_Discovery.pdf

Format Specification Proves Crucial in *Cenveo* Case

By Emily M. Dierberg

In *Cenveo Corp. v. Southern Graphics Systems*,¹ the defendants served the plaintiff with document requests. In their requests, the defendants defined the word “document” to include “electronically stored information in its native format.” Their first request specified that all documents responsive to that request should “be produced in native format with all attachments in native format.” The other requests simply asked for “documents.” The plaintiff thereafter produced documents as Adobe PDF images.

The defendants filed a motion to compel production of the electronically stored documents in native format. The plaintiff argued that the defendants did not define “native format,” and therefore the plaintiff produced the documents “in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms,” as allowed under the Federal Rules where a request fails to specify the format. The court disagreed with the plaintiff’s argument.

In granting the defendants’ motion to compel, the court noted that Rule 34 of the Federal Rules of Civil Procedure permits a party’s request to “specify the form or forms in which electronically stored information is to be produced.” The court found the term “native format” unambiguous, which specified the format for the document production.

The court also examined the advisory notes to Rule 34 which state that “the responding party must state the form it intends to use for producing electronically stored information if the requesting party does not specify a form or if the responding party objects to a form that the requesting party specifies.” Since the plaintiff failed to object or state a form other than “native format,” it was required to re-produce everything in its native format.

The lesson from *Cenveo* clearly indicates that in propounding discovery, a party should specify the format for production. If the responding party fails to object, the production will likely be in the format requested. Responding parties must also carefully review the requests for a specified form. If none is specified, the responding party can choose its own format, which a court will likely respect so long as it is reasonably usable.

A party’s production format can have lasting implications in litigation. Documents in their native format will also likely include metadata and along with this metadata may come potentially damaging revelations of prior deletions or insertions. Document images, on the other hand, only display the document’s final version. Accordingly, strategically specifying the format of your opponent’s production is an important decision that should be decided shortly after the inception of the litigation as it may have significant impact at later stages.

¹ *Cenveo Corp. v. Southern Graphics Sys.*, No. 08-5521, 2009 WL 4042898 (D. Minn. Nov. 18, 2009)

E-Discovery Across International Borders Part Two: U.S. Courts Tackle European Privacy Laws

By Lisa C. Sullivan

Last month, we alerted readers to the thorny issues that may arise when U.S. e-discovery obligations conflict with international privacy laws. This month, we discuss how U.S. courts have dealt with these conflicts.

By now, you know that complying with e-discovery obligations can be complicated if your electronic document collection involves foreign offices. You’re aware of EU Directive 95/46 and the country-specific “blocking statutes” that impact your efforts. You’re also quite cognizant of the importance of complying with your U.S. discovery obligations. At this point, you’re wondering: How have the U.S. courts resolved these issues?

One way to answer this question is: They largely haven’t – at least, not in the specific context of e-discovery. However, the courts have frequently addressed the conflict between U.S. discovery obligations and foreign privacy laws in the context of routine discovery requests. These decisions shed light on the analysis that would likely apply.

Societe Nationale:

U.S. Courts May Order Discovery of Foreign Litigant

The Supreme Court’s decision in *Societe Nationale Industrielle Aerospatiale v. U.S. District Court for the Southern District of Iowa*¹ established that U.S. federal courts have the authority to order a foreign litigant to comply with U.S. discovery obligations. The Court opined that “[i]t is well known that the scope of American discovery is often significantly broader than is permitted in other jurisdictions, and we are satisfied that foreign tribunals will recognize that the final decision on the evidence to be used in litigation conducted in American courts must be made by American courts.”² The Court cautioned, however, that federal courts must “take care to demonstrate due response for any special problem confronted by the foreign litigant” and “should exercise special vigilance to protect foreign litigants from the danger that unnecessary, or unduly burdensome, discovery may place them in a disadvantageous position.”³

Disappointingly, however, the Court declined to “articulate specific rules to guide this delicate task”⁴ (other than to suggest balancing factors relevant to a comity analysis) – leaving it to other courts to address the messy e-discovery issues down the road.

The Relevant Factors

In the wake of *Societe Nationale*, U.S. courts have examined some or all of the following factors in determining whether to order discovery of a foreign party:

- The competing interests of the two countries. (This is sometimes evaluated as the extent to which non-compliance would undermine important interests of the

U.S., or to which compliance with the request would undermine important interests of the foreign country.)

- The hardship of compliance on the party or witness.
- The importance of the discovery to the litigation.
- The good faith of the party resisting discovery.
- The degree of specificity of the discovery request.
- Whether the information originated in the U.S. or in the foreign country.
- Whether alternative means exist to obtain the information.

The vast majority of U.S. courts have ordered discovery after weighing the relevant factors.

The *Credit Lyonnais* Example

For example, in *Strauss v. Credit Lyonnais, S.A.*,⁵ the defendant, a French financial institution, objected to several document requests, interrogatories, and requests for admission based on a French blocking statute. In deciding the plaintiffs' motion to compel, the court weighed each of these factors. The court found the discovery requests to be narrowly-tailored and both relevant and crucial to the litigation,⁶ and held the U.S.'s and France's interests in the subject matter of the lawsuit (combating terrorism) to be aligned and not outweighed by French secrecy laws.⁷ The court also found that the defendant had made good faith efforts to secure discovery—but these efforts did not preclude ordering production.⁸

The most interesting aspect of the court's analysis was the "hardship of compliance" factor. The court recognized that France's blocking statute carried the possibility of both civil and criminal penalties.⁹ Recognizing that the prospect of "criminal penalties rather than civil liabilities weighs in favor of the objecting party," the court also held that this hardship should be accorded less weight if the litigant is a party.¹⁰ Here, the court found it unlikely that France would penalize the defendant for producing discovery: "Glaringly absent from the submission by Credit Lyonnais is any indication that civil or criminal prosecutions by the French government . . . are likely, rather than mere possibilities."¹¹

Some months later, Credit Lyonnais sought a protective order concerning more recent discovery requests.¹² This time, the defendant came armed with a letter from the French Ministry of Justice, a Paris Court of Appeals opinion, and a declaration from a French law expert—all of which detailed the criminal sanctions the defendant could face by responding to the discovery requests.¹³ The court was unmoved, noting that the new documents "added little to the analysis that justifies altering in any significant way the court's prior balancing."¹⁴ Notably, the court observed that "the French Ministry's letter does not state that Credit Lyonnais will be prosecuted if complies with this court's order to provide discovery."¹⁵ The court again ordered discovery.

The court's speculation proved incorrect. The French counsel was criminally prosecuted and fined 10,000 Euros.¹⁶ Even in light of this prosecution, some U.S. courts have continued to find "the chance of prosecution under the French Blocking Statute [to be] minimal."¹⁷

Applicability of the Factors in the E-Discovery Realm

When it comes to e-discovery issues, there is good reason to believe that the factors courts have historically examined will continue to be applied. However, e-discovery can have some twists that make application of the factors difficult.

For example, in the early stages of litigation, parties know about their Rule 26(a)(1) obligations to preserve, and then produce, relevant documents in advance of a request from opposing counsel. Because there is no "discovery request" at issue, it may be more difficult to evaluate the importance of the documents to the litigation. The degree of specificity of the request becomes irrelevant. Detailed discussions with experienced e-discovery counsel will be necessary to determine the scope of production.

Coming next issue: Practical advice on handling international e-discovery issues for both the producing party and the requesting party.

¹ 482 U.S. 522 (1987).

² *Id.* at 542.

³ *Id.* at 546.

⁴ *Id.*

⁵ 242 F.R.D. 199 (E.D.N.Y. 2007).

⁶ *Id.* at 212.

⁷ *Id.* at 214-24.

⁸ *Id.* at 226.

⁹ *Id.* at 224.

¹⁰ *Id.* at 225.

¹¹ *Id.* at 224.

¹² *Strauss v. Credit Lyonnais, S.A.*, 249 F.R.D. 429 (E.D.N.Y. 2008).

¹³ *Id.* at 435-37.

¹⁴ *Id.* at 448.

¹⁵ *Id.* at 449 (emphasis added). This theme echoes in other cases. One court held, "[T]he French blocking statute does not subject defendants to a realistic risk of prosecution." *Bodner v. Paribas*, 202 F.R.D. 370, 375 (E.D.N.Y. 2000). Another court noted, "The majority of courts that have examined the issue have held that France has little interest in the enforcement of its Blocking statute." *In re Vivendi Universal, S.A. Sec. Litig.*, 2006 WL 3378115, at *3 (S.D.N.Y. Nov. 16, 2006). In a case addressing an unidentified country, the court noted that the defendant failed to "present any evidence that the confidentiality asserted . . . is enforced by any active prosecution." *In re Grand Jury Subpoena Dated August 9, 2000*, 218 F. Supp. 2d 544, 563 (S.D.N.Y. 2002).

¹⁶ *In re Advocat "Christopher X"*, No. 07-83228 (Cour de Cassation, Dec. 12, 2007).

¹⁷ *In re Global Power Equip. Group*, 2009 WL 3464212, at *15 (Bkry. D. Del. Oct. 28, 2009).

TECH CORNER

**Collecting E-mail Data for Litigation:
Knowing Where to Look**

By Heidi Goldwater

Most discovery requests include the collection of e-mail. This doesn't mean collecting the entire mail database for a company. Typically, the request will specify data from certain custodians for a particular period of time, or be based on keywords. Sometimes the request includes a variation of both of these items. A common practice in responding to discovery requests for e-mail is for companies to utilize their Information Technology (IT) personnel to collect this data. Depending on the e-mail system in place, this data will most commonly be collected as .pst (Microsoft Exchange) or .nsf (Lotus Notes) files.

When collecting files during discovery, IT personnel need to determine if all of the responsive files have been retrieved. To ensure a complete and comprehensive result, the following searches also should be conducted:

Archive Searches

Archiving functionality is built into e-mail systems. E-mail can be archived to a local drive or a network server, depending on how it is configured by IT personnel. These mail files need to be included when searching for relevant messages to meet the criteria of a discovery request. There are also third party software applications that can assist with archiving or deleting mail prior to a certain date. It is important to note that in addition to understanding archiving, deletion procedures are sometimes configured on e-mail systems and any deletion procedure must be halted during a litigation hold to ensure that all data is collected.

Third Party Application Searches

In addition to corporate mail systems, many employees also use third party e-mail applications such as AOL,

Gmail, or Hotmail to manage their work e-mail. Some employees choose to configure these services to deliver e-mail to their computer hard drive through applications such as Outlook or Outlook Express. If this is the case, collecting the e-mail is fairly simple. If this is not the case, however, you may need to subpoena these companies for the relevant mail. Issuing subpoenas to third parties is oftentimes a lengthy process and should be considered at the initial stages of discovery so deadlines are not missed. If the employee does not configure his or her third party e-mail to be delivered to his or her computer, a forensic consultant may be able to recover remnants of some of the message files in the internet history and cache.

“Deleted” File Searches/Back Up Tapes

Finally, it is important to note that all of an individual custodian's e-mail may not be in his or her current mail file. Aside from archiving, users often delete messages. Messaging systems such as Microsoft Exchange and Lotus Notes are complex and oftentimes deleted mail is retained within the main server database for later retrieval by an administrator. If the systems from which a party is trying to obtain mail don't have these safeguards configured, an alternative option is to search backup tapes if they exist.

E-mail collection requires a good understanding of where the mail is stored prior to acquiring it. IT personnel should be careful when collecting e-mail files for discovery and be certain to utilize the searches outlined above to ensure that all files have been retrieved.

Please visit
www.uhlaw.com/about/contactus
to receive future editions of the
E-Discovery Update via e-mail.

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

Tina B. Solis, Editor	312.977.4482	tbsolis@uhlaw.com
James M. Carlson	312.977.4143	jcarlson@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
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 2010 UNGARETTI & HARRIS LLP
www.uhlaw.com