

Ungaretti & Harris LLP
E-Discovery Update

Inadvertent Productions: What to do if an Error Occurs

By Tina B. Solis

The incorporation of electronically stored information (ESI) into the Federal Rules of Civil Procedure has required the review of massive amounts of information for privilege, responsiveness and other issues prior to production. In many cases, often due to costs issues and time constraints, a party chooses to use an analytical software program, coupled with qualified individuals, to review the mounds of data prior to production. In this context, mistakes can and sometimes do occur. What happens if privileged documents are inadvertently produced? Has a waiver of the privilege occurred? These were the questions recently addressed in *United States v. Sensient Colors, Inc.*¹

In *Sensient*, the plaintiff had produced approximately 45,000 documents to Sensient on six different occasions between May 14, 2008, and February 12, 2009.² On August 29, 2008, Sensient returned 81 documents to the plaintiff that it had deemed privileged.³ On September 10, 2008, the plaintiff sent a letter to Sensient advising it that 80 of the 81 documents were privileged and were inadvertently produced.⁴ On October 23, 2008, Sensient again returned another 89 privileged documents to the plaintiff.⁵ The plaintiff produced a supplemental privilege log on November 21, 2008, claiming that most of the inadvertently produced documents were subject to the attorney-client privilege or work product privilege.⁶ The plaintiff subsequently claimed throughout the following several months that additional documents were inadvertently

produced. Sensient then filed its motion to compel claiming that the plaintiff had waived the privilege with respect to these inadvertent productions.

The Implications of Federal Rule of Evidence 502(b)

The New Jersey District Court, in analyzing whether a waiver had occurred, looked to Rule 502(b) of the Federal Rules of Evidence which was recently amended to state:

Limitations on Waiver

(b) Inadvertent disclosure – When made in a Federal proceeding or to a Federal Office or agency, the disclosure does not operate as a waiver in a Federal or State proceeding if:

1. the disclosure is inadvertent;
2. the holder of the privilege or protection took reasonable steps to prevent disclosure; and
3. the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure 26(b)(5)(b).⁷

The district court applied a two-step analysis to determine whether a waiver occurred. First, the court had to determine whether the documents in question were in fact privileged. Second, if the documents were privileged then a waiver does not occur if the three elements of FRE 502(b) are satisfied. In conducting its analysis, the district court divided the plaintiff's inadvertent production into three groups: (1) documents identified by the plaintiff on September 10, 2008, (2) documents identified in the plaintiff's November 21, 2008, letter, and (3) documents identified by the plaintiff on June 28, 2009, or later.

No Waiver of Privilege for Documents Identified in September 10, 2008 Letter

With respect to the first group of documents identified in the plaintiff's September 10, 2008 letter, the court concluded that the privilege had not been waived. The court noted that the plaintiff's production "was substantial" and that out of the 45,000 pages produced "only a total of 214 are at issue."⁸ The court also found that the privileged information was not self-evident and that the "plaintiff presented substantial evidence that it took reasonable steps to prevent an inadvertent production."⁹ Finally, the court found that a mere eight working days after being informed of the error, the plaintiff notified Sensient that Rule 26(b)(5)(B) should be followed.¹⁰

Waiver of Privilege with Respect to the Last Two Categories of Documents

The court, however, held that the plaintiff had waived the

Contents

Inadvertent Productions:
What to do if an Error Occurs

By Tina B. Solis

Case Analysis:
Southeastern Mechanical Services v. Brody

By Emily M. Dierberg

California's New Meet and Confer Rules:
Addressing E-Discovery Early in Litigation

By Nile N. Park

E-Discovery Across International Borders
Part One: When U.S. Discovery Obligations Confront
European Privacy Laws

By Lisa C. Sullivan

privilege with respect to the second and third categories of documents – namely those in the plaintiff’s November 21, 2008 letter and those identified on June 28, 2009 or later. The court found that plaintiff had satisfied its burden with respect to Rule 502(b)(1) and (2). However, the court stated that the plaintiff did not satisfy the third element because it did not take reasonable steps to rectify the error once it had been placed on notice that “something was amiss with its document production and privilege review.”¹¹ The court found that Sensient’s August 29, 2008 letter should have prompted the plaintiff “to promptly re-assess its procedures and re-check its production.”¹² However, the plaintiff waited almost three months until November 21, 2008 to confirm the error. Moreover, the court found that it appeared that the plaintiff was not even aware of the error until Sensient’s October 23, 2008 letter. In its reprimand of the plaintiff, the court noted:

If [Sensient] was able to discover an error by October 23, 2008, there is no reason plaintiff could not have done the same thing. Indeed, plaintiff had a greater motivation than did [Sensient] to conduct a thorough privilege review after plaintiff confirmed its mistakes on September 10, 2008.¹³

Learning from Sensient

The lesson from the *Sensient* court is easy to discern. Sometimes in productions of this magnitude, mistakes can occur. However, once a party is on notice of a problem with its production and review process, the party is under an obligation to promptly and diligently reassess its procedures to correct the issue. To do otherwise, will likely result in a waiver of the privilege.

¹ *United States v. Sensient Colors, Inc.* 2009 WL 2905474 (D.N.J. Sept. 9, 2009).

² *Id.* at *1

³ *Id.*

⁴ *Id.*

⁵ *Id.*

⁶ *Id.*

⁷ FRE 502(b).

⁸ *Id.* at *4.

⁹ *Id.*

¹⁰ *Id.*

¹¹ *Id.* at *5.

¹² *Id.*

¹³ *Id.*

Case Analysis: *Southeastern Mechanical Services v. Brody*

By Emily M. Dierberg

In *Southeastern Mechanical Services v. Brody*,¹ an employer filed an action against its former employees alleging misappropriation of confidential trade secret information. In the course of discovery, the court ordered the individual defendants to return all employer confidential information, preserve all information on their computers or Blackberry devices regarding the employer, and to refrain from destroying any information relevant to the employer’s claims. Pursuant to the court’s order, the individual defendants returned their

company-issued Blackberry devices and laptops to their employer, who then gave the devices to a forensic computer expert, Jon Kessler, for examination.

After examination, Kessler determined that the Blackberry devices contained no data, including e-mails, text messages, calendar items, telephone records, contacts, attachments, or applications. The parties’ respective experts determined that the data could have been removed from the Blackberry devices by:

1. a data “wipe” by the user;
2. a data “wipe” by a third-party administrator;
3. the user entering an incorrect password ten consecutive times; or
4. Kessler’s inadvertent deletion.

Sanctions Sought Because of Deletion of Blackberry E-mails and Other Data

The employer moved for sanctions against the individual defendants based on their intentional spoliation, or destruction of evidence. The court found it clear that the defendants once had relevant information on their Blackberry devices, including individual e-mails from the defendants’ personal e-mail accounts, which they were obligated to produce. Because that information was deleted, the court had to determine whether the defendants acted in bad faith and destroyed the evidence.

The Court Finds Bad Faith Deletion of Blackberry Data

The court found it was most likely that the “wiped” Blackberry devices were attributable to defendants’ deliberate and intentional actions. The court also found that the circumstances justified a finding that the missing evidence would have been unfavorable to the defendants. The court therefore found that an adverse inference instruction was an appropriate sanction for the defendants’ conduct. It also found that the employer was entitled to a jury instruction that had the defendants preserved such data, it would have been advantageous to the employer and disadvantageous to the individual defendants.

The Lesson About Blackberry Devices

Based on *Brody*, information stored on Blackberry devices and other handheld devices is discoverable and should be preserved once litigation is initiated. If a party doesn’t preserve such information, it risks an adverse inference instruction or worse, a dismissal, as a sanction for its failure to produce. Other courts may also follow the *Brody* court’s reasoning and take an expansive approach to the discoverability of electronically stored information on other mediums. Notably, the *Brody* court recognized that individual e-mails from the defendants’ personal e-mail accounts were discoverable. Litigants should take an expansive approach to preserve all relevant information in the event of litigation.

¹ *Southeastern Mechanical Services v. Brody*, No. 8:08-cv-1151-T-30EAJ, 2009 WL 2883057 (M.D. Fla. Aug. 31, 2009)

California's New Meet and Confer Rules: Addressing E-Discovery Early in Litigation

By Nile N. Park

In many jurisdictions, courts require parties to “meet and confer” early in the litigation process in order to sort out initial disputes and come to some agreements, if possible, regarding the scope of the lawsuit and discovery. Some state courts also have meet and confer requirements. In particular, California recently enacted a meet and confer rule that specifically addresses e-discovery disputes in California state cases.

In conjunction with the June 29, 2009, enactment of California's Electronic Discovery Act, the California Judicial Council amended Rule 3.724 of the California Rules of Court (“CRC”) on August 14, 2009. The purpose of these recent changes was to “improve the procedures for handling the discovery of” electronically stored information and reduce the cost of discovery through proper management.¹

The new CRC 3.724 requires parties to meet and confer by telephone or in person at least 30 days before the initial case management conference to address a number of pre-trial issues. The new CRC 3.724 specifically requires a discussion between all parties regarding the following e-discovery issues:

- preservation of discoverable ESI;
- the form in which the ESI will be produced;
- time in which the ESI will be produced;
- the scope of discovery;
- methods for asserting or preserving claims of privilege and attorney work product, including whether claims of privilege or attorney work product may be asserted after production;
- methods for asserting or preserving claims of confidentiality, privacy, trade secrets, or proprietary status of ESI;
- allocation of cost of producing ESI; and
- any other issues relating to discovery of ESI, including developing a proposed plan.

The purpose of this new rule is to push parties to come to a reasonable agreement regarding e-discovery issues in a case. It is, of course, essential that a party's attorney has a full understanding of the e-discovery issues involved in the lawsuit prior to this meet and confer. A properly prepared attorney should be able to potentially strike an attractive deal with opposing counsel concerning e-discovery.

It is important to note that California courts have the authority to issue case management orders related to Rule 3.724 under Rule 3.728(13). Accordingly, a court may step in and resolve e-discovery issues between parties early in a case before real conflicts about these issues begin. In fact, the amended CRC explicitly forces attorneys to address ESI issues *early* in litigation, a practice that could reduce litigation

costs and future discovery disputes. Proper navigation of the new meet and confer rule, however, requires skilled attorneys who understand the importance of e-discovery issues.

¹ California Courts, Invitation to Comment, Electronic Discovery: Legislation and Rules, No. 08-01, available at <http://www.courtinfo.ca.gov/invitationstocomment/documents/w08-01.pdf>.

E-Discovery Across International Borders Part One: When U.S. Discovery Obligations Confront European Privacy Laws

By Lisa C. Sullivan

You are a U.S. company with offices and computer servers in Europe – and you were just served with a lawsuit in Chicago. You know some relevant documents and e-mails are on your European computer servers, and you know your e-discovery obligations. It's time to start preserving and gathering documents. . . . Or is it? Have you thought about how international privacy and data transfer laws impact e-discovery? Can you collect and produce your European employees' e-mails? Can you disclose information about your European customers?

Maybe not, and acting without consulting counsel could land your company in hot water.

Comparing U.S. Litigation to Foreign Litigation

In U.S. litigation, discovery is broad. The U.S. has one of the most liberal set of discovery procedures. Penalties for non-compliance, especially with respect to e-discovery, can be dire – often, not just monetary sanctions, but case-dispositive sanctions as well (such as adverse inferences or dismissal or default judgment). Moreover, U.S. employees rarely expect that their company e-mails are private. In fact, most companies have written policies making clear that e-mails belong to the employer. Employee e-mails are discoverable, and routinely produced in litigation as part of the e-discovery process.

In other countries, including within the European Union, this is not the case. Discovery is typically much more restrictive than in the U.S. For example, most countries do not have nearly as broad a relevancy standard; even standard document requests may be viewed as overbroad. More importantly, privacy rights and expectations are much stronger in some other countries. As a result, when a U.S. litigant is faced with e-discovery obligations that cross U.S. borders, it is important to be aware of and abide by the information privacy laws of all the countries from which data might be requested.

Foreign Restrictions on Transmitting Data

Many countries, however, have adopted restrictions on transmitting data internationally. For example, the European Union adopted a directive to protect the processing of personal

data (EU Directive 95/46). “Personal data” is a broad concept; it includes any individually-identifiable information. That extends so far as to include an employee’s name and e-mail address. “Processing” is an equally broad term, encompassing the retention and disclosure of data. Businesses may collect, retain, and disclose personal data only (a) to fulfill a specific legitimate purpose, or (b) with the explicit consent of the individual. And, as a general rule, personal data may not be transferred outside the EU to countries deemed not to provide an adequate level of protection.

Further complicating the issue, even within the EU, individual countries may have laws providing additional protection for the privacy of their citizens, such as so-called “blocking statutes” designed to restrict disclosure of information to be used in a foreign litigation. These blocking statutes may impose monetary or other penalties on the transfer of information in response to U.S. discovery requests. In addressing e-discovery issues in Europe, then these blocking statutes must be taken into account as well.

The Potential Fools’ Gold of Safe Harbor Systems

One potential solution is the adoption of a “safe harbor” program. Such a program can minimize some concerns about data transfers between Europe and the U.S. – but it may not solve all issues. For example, the safe harbor program may comply with EU Directive 95/46, but it may not have any impact on a particular country’s blocking statute. In addition, obtaining safe harbor certification can be somewhat cumbersome. The U.S. company must receive certification and must agree to follow several principles relating to data handling. Complicating this issue, because discovery is intended to be shared with the opposing litigant, the safe harbor may not be useful with respect to e-discovery unless the opposing party it also has a safe harbor certification.

What about that “specific consent” exception in EU Directive 95/46? When it comes to employee information, can’t a company avoid the whole problem with a policy requiring employees to agree that their e-mails belong to the company?

Case Study in Foreign Discovery Issues

Obtaining specific consent can sometimes work, as Ungaretti & Harris attorneys have seen. In one lawsuit in which we represented a company in the EU, opposing counsel requested contact information for a former employee – a typical Federal Rule 26(a) disclosure. But the country’s privacy law prohibited disclosure of that information without personal consent. Because the former employee remained on good terms with our client, we were able to obtain his consent to disclose his name and address. We were able to comply with our U.S. discovery obligations while respecting EU law.

But establishing or obtaining consent is not always so simple, especially when it comes to a company-wide policy. First, consent must be freely given and capable of being revoked at any time. That means a policy may have so many employees opting out, and at different times, that it becomes ineffective. Second, some European countries feel that the employer-employee relationship is inherently unequal in terms of the balance of power, and so any “consent” is not freely given. Third, even in those countries that would recognize such consent, that consent may apply only to the personal data of the employee – not to the person with whom your employee is exchanging e-mails.

Lessons in Foreign Discovery

Few U.S. courts have addressed these complications to date. In a future issue of this newsletter, we will analyze those cases and the lessons from those cases. For now, there’s no easy answer when U.S. e-discovery confronts international data transfer laws. The most important thing, however, is to be aware that the issues exist. When discussing initial case management with counsel, you can discuss international discovery issues well before problems arise. Forewarned is forearmed.

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

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
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 2009 UNGARETTI & HARRIS LLP
www.uhlaw.com