April 2008
Volume 13
Issue 3

Hinshaw & Culbertson LLP ■ 222 N. LaSalle Street, Suite 300 ■ Chicago, IL 60601
312-704-3000 ■ www.hinshawlaw.com ■ 312-704-3001
www.lawyeringlaw.com

The Lawyers' Lawyer Newsletter

Recent Developments in Risk Management

Outside Counsel's Affirmative Duties to Oversee Their Clients' Compliance With Discovery Obligations – Duty to Investigate

Qualcomm Inc. v. Broadcom Corp., 2008 WL 66932 (S.D. Cal. Jan. 7, 2008); 2008 WL ___ (S.D. Cal. Mar. 5, 2008)

Risk Management Issue: What is the scope of lawyers' responsibility for supervising their clients' compliance with discovery obligations?

The Case: Qualcomm, Inc., the semiconductor and phone maker, sued its competitor Broadcom, Inc., claiming that Broadcom infringed on Qualcomm's patent rights. Broadcom defended in part by arguing that Qualcomm waived its patent rights by participating in a standards-setting body, the Joint Video Team (JVT), during the relevant time. If Broadcom could demonstrate Qualcomm's participation in the JVT, it would definitively defeat Qualcomm's infringement lawsuit. Qualcomm vigorously denied participating in the JVT.

At trial, Qualcomm continued to deny its participation in the JVT, even when confronted with a document showing a Qualcomm employee, Viji Raveendran, was listed as a member of a JVT group. When one of Qualcomm's lawyers was preparing Ms. Raveendran for her trial testimony, he discovered 21 e-mails on her laptop from the JVT group, but Qualcomm decided the e-mails were not responsive to Broadcom's discovery requests. Qualcomm produced the e-mails at trial only after Ms. Raveendran was forced on cross-examination to admit that she had received e-mails from the JVT group. The jury found in favor of Broadcom, finding that Qualcomm had in fact waived its rights by participating in the JVT. The trial judge ordered Qualcomm to pay some $9 million in attorneys' fees and costs to Broadcom for defending the case.

Months later, a Qualcomm attorney and its general counsel wrote the trial judge, admitting that Qualcomm had found thousands of relevant documents that were not produced, which revealed facts inconsistent with the arguments Qualcomm made at trial. In all, Qualcomm failed to produce more than 46,000 e-mails that fell within the Broadcom discovery requests.

The trial judge ordered Qualcomm's lawyers to appear at a sanctions hearing before the Magistrate Court, at which the Magistrate Court found that Qualcomm had intentionally withheld discovery materials, and that the company could not have done so without its lawyers' assistance. The Magistrate Court rejected the notion that the company hid the documents so effectively that the lawyers did not even know about them, and rejected the possibility that the lawyers were so inept that they just missed the evidence. However, there was no evidence that Qualcomm told the lawyers about the documents, or that the lawyers agreed to conceal them. The Magistrate Court commented it was most likely that the lawyers, all experienced and knowledgeable litigators, suspected the documents existed but chose to ignore the warning signs of suspicious activity.

Some of Qualcomm's lawyers filed timely objections to the Order of the Magistrate Court, and the District Court issued an Order on March 5, 2008, vacating and remanding the Magistrate Court's decision with respect to those attorneys. The District Court held that the "introduction of accusatory adversity between Qualcomm and its retained counsel regarding the issue of assessing responsibility for the failure of discovery, changes the factual basis which supported the court's earlier order denying the self-defense exception to Qualcomm's attorney-client privilege." The District Court went on to state that the "attorneys have a due process right to defend themselves under the totality of the circumstances presented in this sanctions hearing where their alleged conduct regarding discovery is in conflict with that alleged by Qualcomm concerning performance of discovery responsibilities."

Outside Counsel's Affirmative Duties, continued on page 2

HINSHAW & CULBERTSON LLP

Arizona
Victoria Orze
602-631-4400

California
Ronald Mallen
415-362-6000
Frances O'Meara
310-909-8000

Illinois
Thomas Browne
Thomas McGarry
Terrence McAvoy
Jennifer Weller
312-704-3000

Indiana
Renee Mortimer
219-864-5051

Florida
Thomas Sukowicz
954-467-7900
James Sullivan
813-276-1662

Massachusetts
David Grossbaum
617-213-7000

Minnesota
Thomas Kane
Duana Grage
612-333-3434

Missouri
Terese Drew
314-241-2600

New York
Anthony Davis
Hal Lieberman
Philip Touitou
212-935-1100

Oregon
Peter Jarvis
503-243-3243

Rhode Island
David Grossbaum
401-454-7700

Wisconsin
Randal Arnold
414-276-6464

Comment: Qualcomm's outside counsel were hard-pressed to defend themselves at the sanctions hearing before the Magistrate Court because Qualcomm refused to waive the attorney-client privilege and permit the lawyers to explain the facts surrounding the discovery responses. The lawyers were therefore unable to explain who, exactly, was responsible for discovery compliance (as between outside counsel and the client's employees, or general counsel), or what specific steps they took to assure themselves that the client was being forthcoming. Notably, while most jurisdictions' ethics rules permit lawyers to disclose client confidences to the extent necessary to defend themselves in the face of such claims, California's ethical rules do not. However, in vacating and remanding the Magistrate Court's decision, the District Court cited authority, which included A.B.A. Model Rules of Prof. Conduct 1.6(b)(5) & comment 10.

Risk Management Solution: When a law firm takes on complex litigation involving a client, it should, in addition to explaining the rules regarding the requirement of a litigation hold to prevent any document destruction, also seek agreement with the client at the outset regarding the management of the discovery process. The law firm should obtain all litigation clients' written commitment to give the firm full access to the information the firm deems necessary to comply with discovery requests. If the client is reluctant to provide unrestricted access, the law firm should reconsider whether to accept the engagement. At a minimum, if the client wants to maintain control over the discovery process and its results, the firm should require the client's in-house lawyers to personally verify all discovery responses before relying on the responses. However, this does not remove the risks, as it will likely not insulate outside counsel from their obligations, as explained in this case and others (*See,* e.g., *Zubulake v. UBS Warburg,* 2004 WL 1620866 (S.D.N.Y.) In *Zubulake,* Judge Scheindlin described outside counsel's duties as follows:

> "First, counsel must issue a 'litigation hold' at the outset of litigation or whenever litigation is reasonably anticipated. The litigation hold should be periodically re-issued so that new employees are aware of it, and so that it is fresh in the minds of all employees. Second, counsel should communicate directly with the 'key players' in the litigation, i.e., the people identified in a party's initial disclosure and any subsequent supplementation thereto. Because these 'key players' are the 'employees likely to have relevant information,' it is particularly important that the preservation duty be communicated clearly to them. As with the litigation hold, the key players should be periodically reminded that the preservation duty is still in place. Finally, counsel should instruct all employees to produce electronic copies of their relevant active files. Counsel must also make sure that all backup media, which the party is required to retain, is identified and stored in a safe place. In cases involving a small number of relevant backup tapes, counsel might be advised to take physical possession of backup tapes. In other cases, it might make sense for relevant backup tapes to be segregated and placed in storage. Regardless of what particular arrangement counsel chooses to employ, the point is to separate relevant backup tapes from others. One of the primary reasons that electronic data is lost is ineffective communication with information technology personnel. By taking possession of, or otherwise safeguarding, all potentially relevant backup tapes, counsel eliminates the possibility that such tapes will be inadvertently recycled." [citations omitted])

To address these issues, some law firms have established special teams within their litigation practice groups to assist lawyers with electronic discovery issues and to ensure compliance with the obligations imposed by the courts.

Use of Employer's E-mail System to Communicate With Counsel May Result in Loss of Attorney-Client Privilege and Work Product Protection

Scott v. Beth Israel Medical Center Inc., 2007 WL 3053351 (N.Y. Sup. Oct. 17, 2007)

Risk Management Issue: What are a lawyer's duties regarding preservation of the attorney-client privilege and work product protection when communicating with a client via e-mail? In particular, are there special duties when the lawyer is aware that the client is using an e-mail address controlled by a third party, such as the client's employer?

The Case: Plaintiff Dr. W. Norman Scott brought this breach of contract action against his former employer, Beth Israel Medical Center Inc., arising from the termination of his employment. After learning from counsel for Beth Israel that it was in possession of e-mail correspondence between plaintiff and his counsel that had been transmitted utilizing Beth Israel's email system, plaintiff moved for a protective order requiring Beth Israel to return all such e-mail correspondence. Plaintiff asserted both the attorney-client privilege and work product doctrine in support of his motion for protective order.

Beth Israel countered that the e-mails were never protected by the attorney-client privilege because plaintiff could not have made the communications in confidence when using Beth Israel's e-mail system, as such use was in violation of Beth Israel's e-mail policy. That policy stated: "[a]ll Medical Center computer systems . . . electronic mail systems, Internet access systems, . . . and the wired or wireless networks that connect them are the property of the Medical Center and should be used for business purposes only." Additionally, "[a]ll information and documents created, received, saved or sent on the Medical Center's computer or communications systems are [sic] of the Medical Center. Employees have no personal privacy right in any material created, received, saved or sent using Medical Center communication or computer systems. The Medical Center reserves the right to access and disclose such material at any time without prior notice."

After reviewing the facts, and concluding that the plaintiff either had actual knowledge of the policy, or had constructive knowledge by virtue of his position as an administrator, the court analyzed the attorney-client privilege claim upon the authority presented in *In re Asia Global Crossing, Ltd.,* 322 B.R. 247 (S.D.N.Y. 2005). The *Asia Global Crossing* court concluded that the attorney-client privilege is inapplicable if: "(a) ... the corporation maintain[s] a policy banning personal or other objectionable use, (b) ... the company monitor[s] the use of the employee's computer or email, (c) ... third parties have a right of access to the computer or emails, and (d) ... the corporation notif[ies] the employee, or was the employee aware, of the use and monitoring policies."

Determining that all of these tests were satisfied, the court held that plaintiff's use of his employer's e-mail system to communicate with his attorney in violation of Beth Israel's policy renders the communication not made in confidence and thus destroyed the attorney-client privilege, if it ever applied. As with any other confidential communication, the holder of the privilege and his or her attorney must protect the privileged communications, otherwise, the privilege is waived. The court reasoned that the effect of an employer e-mail policy, such as that of Beth Israel, is akin to having the employer looking over the employee's shoulder each time an e-mail is sent, and therefore, plaintiff's messages could not have been made in confidence.

With regard to plaintiff's contention that the e-mails were privileged work product, the court noted that while inadvertent production of a privileged work product documents generally does not waive the applicable privilege, an exception is made where a party's conduct is "so careless as to suggest that it was not concerned with [the] protection of [the] asserted privilege." Critical to such a determination is the reasonableness of the precautions taken to prevent inadvertent disclosure.

Plaintiff argued that reasonable precautions were, in fact, taken based upon the following notice, which was included in every e-mail sent to plaintiff from his counsel: "[t]his message is intended only for the use of the Addressee and may contain information that is privileged and confidential. If you are not the intended recipient, you are hereby notified that any dissemination of this communication is strictly prohibited. If you have received this communication in error, please erase all copies of the message and its attachments and notify us immediately."

However, the court concluded that this "notice cannot create a right to confidentiality out of whole cloth" and that the "notice might be sufficient to protect a privilege if one existed" but cannot alter Beth Israel's email policy. "When client confidences are at risk, [the law firm's] *pro forma* notice at the end of the e-mail is insufficient and not a reasonable precaution to protect its clients."

Risk Management Solution: This decision sends an important message to lawyers about the need to give all clients explicit advice at the outset of every representation regarding the use of e-mails for communications that the client or the lawyer wish to have treated as confidential. Neither the client nor the lawyer should be using emails through any server or site as to which there is no reasonable expectation of confidentiality. And as the case makes plain, this includes all employer systems where the employer has expressed and circulated a "no personal use" or no expectation of privacy policy. Put another way, this case suggests the need to add a paragraph to all engagement letters to warn clients of this issue, and to provide advice as to the form that all communications need to take in order to preserve confidentiality.

Failure to Preserve Temporary Internet Cache Files Did Not Warrant an Adverse Spoilation Inference

Health Care Advocates, Inc. v. Harding, Earley, Follmer & Frailey, 2007 WL 208358 (E.D. Pa. July 20, 2007)

Risk Management Issue: What obligation does counsel have to preserve electronically stored information that is inadvertently collected?

The Opinion: Health Care Advocates was the plaintiff in a lawsuit alleging that a certain competitor of the company infringed upon trademarks and misappropriated trade secrets. The Harding firm represented the defendants in that lawsuit, which was dismissed on summary judgment.

After the dismissal, Health Care Advocates filed a separate action against the Harding firm concerning events that occurred in the prediscovery phase of the underlying litigation. Health Care Advocates alleged that the Harding firm's investigation of the underlying litigation in accessing a previous incarnation of Health Care Advocates' web site violated various federal laws, including the Digital Millenium Copyright Act.

The Harding firm's investigation of the underlying litigation lead it to search the Internet for information about Health Care Advocates. Employees of the Harding firm accessed the web site operated by the Internet Archive, www.archive.org, and viewed archived screen shots of Health Care Advocates' web site via a tool contained on Internet Archives' web site called the "Wayback Machine." The Wayback Machine allowed the Harding firm to see what Health Care Advocates' public web site looked like prior to the date the complaint was filed in the underlying litigation.

The Harding firm utilized the contents of Health Care Advocates' archived web site to assess the merits of the claims in the underlying litigation, which were brought against the firm's clients. While the Harding firm printed copies of each archived screen shot of Health Care Advocates' public web site, they did not actively save any such information onto their computer hard drives. However, when the Harding firm viewed archived screen shots of Health Care Advocates' web site through the Wayback Machine, copies of the screen shots may have been automatically stored in the cache files of the Harding firm's computers. The Harding firm made no effort to preserve these temporary files immediately after they used their web browsers.

In granting summary judgment to the Harding firm, the court also rejected Health Care Advocates' request for spoilation sanctions based upon the Harding firm's failure to preserve the temporary cache files that were involuntarily saved to the firm's computers. The court applied a three-part balancing test to evaluate whether sanctions were appropriate based upon the loss of evidence. The court considered: 1) the degree of fault of the party who altered or destroyed the evidence; 2) the degree of prejudice suffered by the opposing party; and, 3) whether there was a lesser sanction that would avoid substantial unfairness to the opposing party, and where the offending party is seriously at fault, would serve to deter such conduct by others in the future. *Schmid v. Milwaukee Elec. Tool Corp.,* 13 F.3d 76, 78 (3rd Cir. 1994).

With regard to the first consideration, the court stated that "very little fault can be attributed to the Harding firm for the loss of these temporary cache files" and noted that "the most important fact regarding the loss of evidence is that the Harding firm did not affirmatively destroy the evidence" due to the fact that the cache files were deleted from the Harding firm's computers automatically. Further, the court found that the Harding firm had no reason to anticipate that using a public web site to view images of another public web site would subject them to a civil lawsuit containing allegations of hacking, or that the temporary cache files would be sought.

Regarding the second and third considerations, the court also concluded that Health Care Advocates suffered very little prejudice due to the lost evidence, and because the Harding firm did not purposely destroy evidence, to "impose a sanction on the Harding firm for not preserving temporary files that were not requested, and might have been lost the second another web site was visited, does not seem to be a proper situation for an adverse spoilation inference."

Risk Management Solution: Although the issue arises in a different manner, this case further emphasizes the need for law firms to develop the experience necessary for the proper management of electronic discovery and act reasonably when addressing these issues. Lawyers must be mindful of the electronically stored information that is generated during the course of their work and their corresponding duty of preservation.

Metadata Ethics Opinion – Arizona Adopts the Position of Florida, New York and Alabama

Arizona Bar Association Opinion 07-03: Confidentiality; Electronic Communications; Inadvertent Disclosure (Nov. 2007)

Risk Management Issue: What precautions must a law firm take in order to prevent the disclosure of privileged metadata? What steps must a recipient of inadvertently produced metadata take upon the receipt of such information? And is "data mining" permissible?

The Opinion: Arizona Bar Association Opinion 07-03 addresses the ethical duties of lawyers who send and receive electronic communications, which may contain metadata. As noted in the Opinion, "[b]y 'mining' the metadata in a document, it may be possible to identify the author of the document, the changes made to the document during the various stages of its preparation and revision, comments made by the persons who prepared or reviewed the document, and other documents embedded within the document."

With regard to the sender of electronic communications, lawyers must take reasonable precautions to prevent inadvertent disclosure of confidential information. "What is 'reasonable' in the circumstances depends on the sensitivity of the information, the potential consequences of its inadvertent disclosure, whether further disclosure is restricted by statute, protective order, or confidentiality agreement, and any special instructions given by the client." While reasonable precautions must be taken to scrub metadata from electronic documents, when "removing or restricting access to metadata in documents produced or disclosed in litigation, the lawyer must take care not to violate any duty of disclosure to which the lawyer or the lawyer's client is subject."

With regard to recipients of electronic communications, Arizona joined Florida, New York, and Alabama in taking the position that a lawyer receiving an electronic document should not try to obtain information from metadata that the lawyer knows or should know is not intended for the receiving lawyer. If the recipient discovers metadata by any means, and knows or reasonably should know that the sender did not intend to transmit the information, the recipient has a duty to notify the sender. Noting that American Bar Association Formal Op. 06-442 concluded that the Model Rules of Professional Conduct do not prohibit such conduct, Arizona respectfully declined to adopt that position, reasoning that even "[d]espite the most reasonable and thorough precautions . . . it may not be possible for the sending lawyer to be absolutely certain that all of the potentially harmful metadata has been 'scrubbed' from the document before it is transmitted electronically."

Except in very specific circumstances, such as when an opponent consents or other law or rule (such as a discovery order) allows it, "a lawyer who receives an electronic communication may not examine it for the purpose of discovering the metadata embedded in it." Further, the recipient lawyer has a duty not to "mine" the document for metadata that may be embedded therein or otherwise engage in conduct which amounts to an unjustified intrusion into the client-lawyer relationship that exists between the opposing party and his or her counsel.

Comment: The view on this issue taken by Arizona, Florida, New York, and Alabama is problematic in that a heightened obligation is imposed upon a lawyer, which is different from that imposed upon the client, were the client to receive and/or possess an electronic copy of the same document. The ABA's position, as adopted by the Maryland State Bar Association, Ethics Docket No. 2007-09, provides what appears to be the superior position as to these issues.

Risk Management Solution: With respect to the transmission of documents electronically, as expressly noted in the Opinion, "Lawyers who send communications or other documents electronically must be aware that such activity has inherent risks . . . [and] must take reasonable measures to prevent the inadvertent disclosure of confidential client information." Firms can assist their lawyers in complying with this admonition by providing automatic "scrubbing" software to "cleanse" documents about to be transmitted electronically, and by providing additional software to enable documents to be saved in ".pdf" rather than word-processing format before transmission, and by training all attorneys and staff in the uses of these tools – and why it matters. While reasonable precautions must be taken in every instance, the obligation of the recipient of inadvertently disclosed metadata and Arizona's prohibition against data mining continues to be a dynamic area of the law and varies from one jurisdiction to the next. *C.f. District of Columbia, Op.* 341 (September 2007) (holding that "[a] receiving lawyer is prohibited from reviewing metadata sent by an adversary *only* where he has actual knowledge that the metadata was inadvertently sent.") (Emphasis added).