

July 11, 2008

ALM

IN-HOUSE COUNSEL

Minimizing the Risk That E-Discovery Failures Will Create Corporate Liability

KIRBY BEHRE AND MARK KOEHN

SPECIAL TO LAW.COM

JULY 11, 2008

E-discovery practice in civil cases and government investigations has rapidly evolved since the onset of federal rules governing electronic discovery a little over a year ago. During its infancy, e-discovery was viewed as a costly but powerful tool that could generate "smoking gun" emails that would alter the outcome of cases. Just a few years ago, litigants were infrequently sanctioned for e-discovery failures, in part, because many judges gave litigants who botched e-discovery the benefit of the doubt and chalked up e-discovery mishaps to "the learning curve." Those days are over.

Judicial tolerance for shortcomings in e-discovery is on the decline, and litigants, their counsel and e-discovery vendors are facing direct liability for such failures. As a result, sensibly managing e-discovery is critical not only to success in the underlying litigation but to minimizing the possibility that e-discovery failures will become a source of liability in and of themselves. Before reviewing some ways to minimize the risk that e-discovery failures will create liability, this article draws upon two recent and notable e-discovery disputes to show how liability can arise.

LIABILITY FOR FAILURE TO DISCOVER AND PRODUCE ELECTRONIC EVIDENCE

In early January 2008, a court ordered Qualcomm to pay Broadcom over \$8.5 million in attorney fees and costs

for discovery abuses in Qualcomm's patent suit against Broadcom, referred six of Qualcomm's outside counsel to the State Bar of California for further investigation and possible sanction, and ordered the six outside counsel to collaborate with five of Qualcomm's in-house counsel to draft a case management protocol to serve as a model for the future. The court awarded this remarkable sanction to address what it characterized as a "monumental discovery violation[.]" Qualcomm's "intentional[l withholding of] tens of thousands of decisive documents" that could not have been achieved "without some type of assistance or deliberate ignorance from its retained attorneys." The documents included emails and other electronic documents demonstrating that, contrary to Qualcomm's stated litigation position, Qualcomm had participated in developing an industry standard which would lead to infringement of Qualcomm's patents.

The court identified "numerous warning flags" that should have led to discovery and production of the withheld documents, including: (1) Broadcom's production of an "email reflector list" showing that email regarding the standard-setting activity may have been sent to Qualcomm's employees early on during the standard drafting process; (2) Broadcom's impeachment of multiple Qualcomm Rule 30(b)(6) witnesses with documents showing Qualcomm's involvement in early stages of the standard-setting activity; and (3) Qualcomm's eve of trial discovery of nearly two dozen emails showing Qualcomm's involvement early in the standard drafting process. The court also noted Qualcomm's specific failures to act, including: (1) failure to search the computers of its

Rule 30(b)(6) witnesses for responsive email and other documents; (2) failure to use search terms that could have been derived from the "email reflector list" produced by Broadcom; and (3) failure to otherwise access and review the computers, databases and emails of its employees and consultant involved in the standard-setting process.

LIABILITY FOR FAILURE TO QUALITY CHECK E-DISCOVERY DELIVERABLES AND ADEQUATELY COMMUNICATE ABOUT E-DISCOVERY PROGRESS

In late December 2007, disappointed with e-discovery services from a well-known e-discovery vendor, a prominent law firm sued the e-discovery vendor seeking a declaratory judgment that the vendor breached its contract with the law firm and that the law firm did not owe the vendor for the approximately \$700,000 in outstanding invoices. Ten days later, the vendor responded with its own lawsuit seeking full payment plus interest. The law firm and vendor quickly announced that they had reached a settlement.

The law firm's complaint alleged breach due to the vendor's: (1) delays in loading data for review by the law firm; (2) failure to keep the law firm informed of when data and the volume of data that would be ready for review by the law firm; (3) missing deadlines for providing CD-ROMs and other media to the law firm for production; and (4) lack of quality control, such as providing for production by the law firm documents previously flagged as non-responsive or requiring additional review by the law firm. These are common complaints, and law firms will increasingly hold vendors accountable for quality shortcomings in the future.

E-DISCOVERY LIABILITY TO THE DISCOVERY RESPONDENT, ITS LAW FIRM, AND E-DISCOVERY VENDOR

The recent Qualcomm-Broadcom and law firm-vendor e-discovery squabbles foreshadow the shape of e-discovery disputes to come: disputes in which the e-discovery failures provide their own source of liability to all stakeholders in the e-discovery process. For instance, what if in the Qualcomm case, all or part of the discovery failures could fairly be laid at the feet of an e-discovery vendor rather than the client or its counsel? Qualcomm

and/or its outside counsel would have a claim against the vendor for all or part of any sanctions award or other adverse result, provided the contract with the vendor did not limit liability. Similarly, what if a vendor's e-discovery failures caused a law firm's client to miss a crucial discovery deadline or lead to irreversible disclosure of attorney-client privileged or other protected information? The client might have a malpractice claim against the law firm and the e-discovery vendor might bear a portion of the ultimate liability.

Such potentially far reaching e-discovery liability simply has no counterpart in the bygone days of paper discovery. Without expertise and resources from an e-discovery vendor, clients and law firms are generally ill-equipped to navigate and produce responsive information from the client's computer systems. Moreover, an e-discovery vendor's technical glitches may quickly turn into potentially case threatening events.

HOW TO MINIMIZE THE POTENTIAL FOR E-DISCOVERY LIABILITY

One e-discovery vendor commenting on the Qualcomm debacle concluded that the court's sanction ruling provided "a lesson in why it's so important to produce every bit of electronic evidence." Clearly, that is not the lesson of *Qualcomm*. *Qualcomm* illustrates the duty to identify and produce the results of "reasonable inquiry" as required by the federal rules. In order to meet that obligation and minimize the potential liability for e-discovery failures, the following considerations are key:

Minimize Data Loss. Identify and preserve the static media (e.g., backup tapes) expected to have the oldest potentially relevant e-documents. In most cases, this should be done as soon as possible after learning of the potential for litigation since static media is often subject to recycling or overwriting in the normal course.

Identifying and preserving potentially relevant static media more often involves extensive discussion with the discovery respondent's in-house IT staff and the relevant business leaders or custodians. The business leaders and custodians help identify the kinds of e-documents (including databases as well as word-processed documents and email) and where they understand them to be stored from an end-users' perspective. After such identification, the IT staff should be able to identify the resources used

behind the scenes to maintain such e-documents (e.g., names of particular computer servers, etc.) and the available static media on which backups may be found.

Remember, however, the resources used to maintain a major business's various e-documents are almost always in flux. Servers may be routinely overwritten and redeployed as the business needs change. Some servers crash and must be replaced or rebuilt. E-documents stored on one set of servers a year ago may now reside on other servers as data storage is balanced across the system. New software is implemented and old software taken offline – often necessitating data conversions and use of temporary storage devices and sometimes involving planned data destruction. As a result, identifying and preserving the static media expected to have the oldest potentially relevant documents can take days, weeks or maybe longer.

In determining the extent to which other static media should be preserved, consider whether such media is expected to contain potentially relevant e-documents not available on active media (i.e., computer hard drives in daily use) or on the static media expected to have the oldest potentially relevant e-documents. Frequently, and for the reasons described in the section below on "sensible transparency," these determinations are best informed by substantive meet and confer with the discovery proponent.

With respect to active media, identify and preserve the relevant contents of desktop and laptop computers used by key custodians – those personnel most likely to be targeted as witnesses – including corporate representatives. As the recent Qualcomm decision underscores, the fallout from failing to preserve and then search the computers of Rule 30(b)(6) witnesses for responsive email and other documents may be devastating.

Minimize Data Ignorance. Although it is generally cost prohibitive to index and run key word searches on the contents of all static and active media, consider other options for minimizing ignorance about the e-documents actually preserved. Other options include:

File Extension Reports. These reports are usually generated relative to a particular item of media (e.g., a particular server or hard drive backup) and list each unique file extension or type (e.g., ".doc", ".pdf", ".xls", etc.) found on the media, a brief description of what such

file extension are typically used for, the total number of such files on the media, the total file size (usually expressed in byte size – e.g., MBs or KBs), and the average size per file. Such reports give a quick "heads up" as to the sheer volume of files that may be expected to contain potentially responsive e-documents.

Path Name/File Name Reports. These reports also are usually generated relative to a particular item of media and list file directory information, such as path name and file name (e.g., "C:/Documents and Settings/My Documents/ABC Project/Project Team Org Chart.doc") and file size, as well as some file "meta-data", such as creation date, last modified date, author name, etc. Such reports give a useful overview of files that may be expected to contain potentially responsive e-documents – especially if path name and file names are expected to be descriptive of file contents. Obtaining such reports in spreadsheet form is preferred so that sort and search features can be used to identify, for instance, all files authored by a particular person or modified during a particular period.

Sampling Searches. These key word searches are run on a sampling of the various items of media that have been preserved. In selecting particular items of media for sampling searches, consider how to best create one or more "cross sections" of such media. For instance, select items of media expected to contain (i) the oldest and newest e-documents as well as some dated in between or (ii) e-documents from several key custodians or custodians from several key business areas of interest.

The focus of sampling searches is less to identify particular documents for production and more to identify the particular key words and key word combinations likely to be useful in later searching efforts on other media. Such searching often involves "iteration" in which new potential key words are identified and used based upon review of potentially relevant documents identified through earlier searches. This is another area where "sensible transparency" to the discovery proponent and substantive meet and confer may help to minimize accusations of withholding based on reckless or willful ignorance. Consider asking the discovery proponent for any key words the discovery proponent may want used.

Anticipate and Prepare for Inevitable Glitches. Remain cautious and prudently skeptical in identifying, preserving, reviewing, and producing e-documents. For example, if

the discovery proponent has been promised a list of all preserved media available for further review, check to make sure such media is in physical possession and do not simply rely upon a backup tape listing prepared by in-house IT staff in the normal course of business. While the discovery respondent may have high confidence that procedures are followed and backup tapes are available as expected – such procedures are rarely put to the test until a catastrophic system crash occurs or, of course, the need to respond in litigation. In-house IT staff is only one source of potential glitches. Unless flagged early for backup by the discovery respondent's counsel, a departing custodian's laptop may be overwritten and redeployed. A miscommunication between counsel and an e-discovery vendor may result in production of information that should be withheld or withholding of information that should be produced.

In all discovery efforts, reasonable diligence and reasonable inquiry is required. As a practical matter, because unexpected e-discovery glitches will occur and may be difficult to articulate and justify if challenged, investing more than reasonable efforts may be a prudent strategy for avoiding unexpected glitches and the best preparation for when they do occur. More than reasonable efforts, of course, does not necessarily translate into more documents produced. As the court in *Qualcomm* noted, "Producing 1.2 million pages of marginally relevant documents while hiding 46,000 critically important ones does not constitute good faith and does not satisfy either the client's or attorney's discovery obligations." *Qualcomm Inc. v. Broadcom Corp.*, Case No. 05cv1958-B (BLM), LEXSEE 2008 U.S. DIST. LEXIS 911 at *31 (S.D. Cal. Jan. 7, 2008).

Support Sensible Transparency. As discovery deadlines approach, a party may be able to obtain additional discovery, sanctions, or even issue or case dispositive inferences – despite the discovery respondent's reasonably diligent efforts to "turn square corners" and provide responsive discovery. Sensible transparency – with opposing counsel and the court – may be the best strategy for minimizing the risk of this result. "Sensible transparency" means sharing sufficient information to engaging in substantive meet and confer aimed to achieve a fair discovery response that avoids undue burden. What should be shared in any case will depend

upon the facts and circumstances but may include, for example, lists of media preserved for potential further review along with descriptions of the expected contents of each item of media, organizational charts and logical diagrams of the discovery respondent's computer systems or relevant portions of them, file extension reports, path name/file name reports, and sampling search results – as described above. Other information that might be shared includes e-discovery vendor pricing for various kinds of further analysis of the media preserved and, if possible, estimated time frames for e-discovery processing and pre-production review.

The goal of sharing at least some such information with the discovery proponent is to determine the contours of a reasonable production effort in advance and avoid later arguments that something more or different should have been done based upon eve-of-trial hindsight. In many cases, far more media is preserved than can possibly be reasonably reviewed for timely production. Information concerning the "metrics" involved in getting the job done may go a long way toward getting the discovery proponent focused on what it really wants. The less the discovery proponent knows about the effort and process, the more likely the discovery proponent will insist on efforts that go beyond reason.

With the court, "sensible transparency" means sharing sufficient information for the court to fairly respond to any discovery proponents' accusations about foot-dragging or improper withholding. Despite the growing number of court decisions resolving e-discovery disputes and various efforts to educate the judiciary and practitioners alike (including those by the Sedona Conference and Georgetown Law Center's Advanced E-Discovery Institute), few judges can be expected to understand or have significant experience with the complexities and burdens of e-discovery. Even if they understand the issues generally, they will have to be educated about the specifics of your case, which will vary widely given the enormous difference in electronic records retentions across various companies and situations.

In sharing sufficient e-discovery information with the court, timing and level of detail is very important. If the discovery proponent is unreasonable in meet and confer and a sensible approach to e-discovery cannot be reached through compromise, consider moving for a

status conference with the judge. Often such conference requests are referred to magistrate judges who sometimes have more "hands-on" experience with e-discovery. Consider also moving for appointment of a special e-discovery master. Often such motions alone will pressure an unreasonable discovery proponent to compromise. Alerting the court to e-discovery issues through such motions practice and/or conferences can be invaluable in defense of any later motions to compel or for sanctions or inferences. In all such communications with the court, strive for concise but accurate explanations and be sure to include information about volume and cost of production to date – including with respect to paper documents. Courts routinely use such information to gauge the reasonableness of e-discovery efforts.

Monitor And Adjust. One lesson, which is too often learned "the hard way," is to monitor and adjust e-discovery efforts throughout the process. Insufficient monitoring and adjusting often results in disputes between discovery respondents and their e-discovery vendor and sometimes causes disputes with the discovery proponent or draws concern from the court. For example, in the Qualcomm case, the court identified "numerous warning flags" that should have led to adjustments in Qualcomm's discovery efforts.

Adequate monitoring involves keeping apprised of custodian interviews that may identify new sources of potentially relevant e-documents as well as IT staff whose assistance may reveal sources previously thought to be destroyed or overwritten. It also often involves day-to-day discussions with the e-discovery vendor hired to process the preserved media into databases used to review and capture attorney impressions before making production and privilege logging decisions. For each step in the process, at least one senior attorney should understand precisely what the e-discovery vendor is doing, how long the effort is anticipated to take, how much it is anticipated to cost, and the anticipated volume of reviewable information available at the end of the step. More and more frequently, discovery respondents that anticipate thorny e-discovery challenges retain experienced e-discovery counsel who may be separate from primary trial counsel.

Making adjustments based upon new information also is critical to minimizing risk and avoiding unnecessary cost. In determining whether and what adjustments may

be sensible, the following questions may be helpful:

- Of all items of media that could be subject to further analysis, are the particular items of media currently in process or under review still the highest priority items?
- For each highly relevant document identified during pre-production review, has the document been reviewed for potentially new key words that might be added to search procedures?
- For each new highly relevant document custodian identified, has the custodian been interviewed about his or her knowledge of likely locations of potentially relevant documents and have efforts been made to identify and preserve documents from any newly identified locations?
- Should the number of attorneys or other document reviewers be increased or decreased and should their task lists and/or search and review procedures be adjusted?
- Would the discovery proponent agree that the adjustments about to be implemented are reasonable under the circumstances?
- Would it be sensible to share any new information with the discovery proponent, including with respect to timing of anticipated production?

At minimum, when faced with new information, consider whether the failure to make any adjustments in the current approach for providing responsive e-discovery could, with later hindsight, be characterized as unreasonable or worse.

Kirby Behre and Mark Koehn practice in the litigation group at Paul, Hastings, Janofsky & Walker LLP. Behre co-chairs the firm's e-discovery group and is a former federal prosecutor and trial lawyer who has practiced criminal, civil and government contract law for the past 21 years. Koehn is a former IT consultant turned litigator who specializes in patent and complex IP and technology disputes. The statements and opinions expressed in this article are not those of the firm or its clients.