MILLER CANFIELD

E-DISCOVERY + RECORDS MANAGEMENT NEWSLETTER

JULY 2012

Google's Privilege Claim: A Cautionary Tale

Winnie the Pooh feared the Heffalumps and Woozles that he believed inhabited the Hundred Acre Wood, although he never saw one. There are things that lurk in the woods of e-discovery that lawyers can't see either… like the auto-save. Although unseen, some unfortunate lawyers for corporate giant Google recently felt its bite.

GOOGLE AND THE AUTO-SAVE

In August 2010, Oracle America filed a patent infringement action against Google alleging that Google's Android smart phone platform infringed certain patents related to Oracle's Java-based smart phone platform. During the course of discovery, Google produced over 3.7 million electronic documents totaling over 19 million pages to Oracle. Within this massive amount of produced electronic records were eight draft versions of an email authored by a Google engineer after attending a strategy meeting called by Google's general counsel regarding Oracle's claims. The final version of this email included the headings "Attorney Work Product" and "Google Confidential," and was sent to Google's senior in-house counsel and a corporate officer and was copied to another Google engineer and the author himself. This final version was withheld from production and appeared on Google's privilege log. Unfortunately for Google, the eight draft versions did not contain the headings and the recipient names were not yet added. This allowed the drafts to escape detection prior to production.

Where did these drafts come from? The record revealed that during the five minutes it took to draft and send the email, Google's Gmail email system automatically saved eight "snapshots" of the email and put the copies into the author's draft email folder. No action was required by the author. It was all done by the auto-save.

When Google learned that it had inadvertently produced draft versions of the email to Oracle, it requested that Oracle return all copies. Oracle complied, but filed a motion to compel production of the draft and final versions of the email. Oracle successfully convinced the district court that the email was not protected by any privilege, and the court ordered the production of all versions of the email. Google sought a writ of mandamus to have the district court's ruling overturned, but the Court of Appeals for the Federal Circuit denied the writ. Even though it was ultimately determined that the Google engineer's email was a non-privileged business communication, there are several significant lessons to be learned from Google's encounter with the auto-save.

SHOULD YOU FEAR THE AUTO-SAVE? ASK IT!

As the *Google* case suggests, in the world of e-discovery, it has become increasingly important to talk to the IT department before any data is identified, collected, processed, reviewed and produced. Google's counsel should have interviewed an IT Department representative to learn what features or systems were in place that could impact the discovery process. A series of questions could have been asked to determine how Google's Gmail system worked. Does the system auto-save drafts? What happens to the drafts once the final email is sent? Where are the drafts stored? Answers to these questions would have alerted counsel to the possible presence of draft versions of sensitive and potentially privileged emails.

Moreover, these types of questions should be asked for other office productivity software as well. Word processing, spreadsheet, and presentation software also may auto-save drafts or create backup versions of files during editing. Knowing if these features exist and how they operate can provide valuable information that can be used during the e-discovery process. For example, knowing that auto-saved drafts or backups of a privileged or otherwise confidential document may exist, lawyers can then use targeted searches to ferret out the drafts.

IT SAYS IT'S PRIVILEGED. THAT'S ENOUGH, RIGHT?

Wrong. It doesn't matter what labels are placed on the document. A grocery list doesn't become privileged because you write "Attorney-Client Communication" on it. As the appellate court made clear in the *Google* case, the contents and context of the communication are determinative when assessing privilege. The court found that the email at issue was a response to a question from Google's management that addressed business rather than legal matters regardless of how it was labeled internally. That does not mean to suggest that placing privilege labels on documents isn't helpful. It certainly can be when it comes to identifying possible privileged communications. But again, the privilege analysis cannot end with the label.

BUT I SENT IT TO A LAWYER!

The fact that a lawyer is a recipient doesn't by itself protect the communication from disclosure. Like a privilege label, the fact that a communication was sent to a lawyer standing alone does not render the communication privileged. If it did, every written or electronic communication would include a lawyer's name, and the truth seeking process would be severely crippled. The appellate court went beyond the "who" and focused on the "what" to determine that the email concerned business not legal matters.

■ **B. Jay Yelton III** +1.269.383.5819

■ **Kenneth J. Treece** +1.269.393.5810

Duty to Preserve: Third Parties

The duty to preserve potentially relevant evidence arises in every lawsuit or government investigation. The scope of the duty, especially in e-discovery, has given rise to myriad opinions. Most litigants are familiar enough to know that when litigation arises or becomes reasonably foreseeable, the duty to preserve commences and they must identify and preserve sources of potentially relevant data in their possession. This is fine as far as it goes. However, litigants must also preserve data within their custody or control. Sometimes, the duty extends to data being held by third parties as discussed in a recent case.

In *GenOn Mid-Atlantic v Stone & Webster, Inc.,* GenOn and Shaw entered into an agreement requiring Shaw to design and build air quality control systems at three GenOn power plants. The agreement did not specify a fixed price, but rather provided a formula based on a comparison of Shaw's actual costs to a target cost. The agreement also gave GenOn the right to audit Shaw's requests for payment under the agreement. In 2009 GenOn hired FTI, a third-party consultant, to conduct the audit. Based on the results of the FTI audit, GenOn filed for a declaratory judgment against Shaw that GenOn owed no additional payments to Shaw under their agreement. At the time it decided to file suit, GenOn made no request to FTI to preserve any audit-related data. Shaw subpoenaed FTI for its audit-related papers and made similar requests for production to GenOn. Shaw received productions from both GenOn and FTI.

Shaw examined the productions and discovered that GenOn had produced email communications with FTI going back to 2009. In contrast, FTI did not produce any email communications with GenOn earlier than March 2010. Shaw's counsel inquired about the discrepancy and was informed by FTI's counsel that it had produced all email communications which it retained in the regular course of business. During subsequent depositions, Shaw learned that FTI had an email retention policy. On a monthly basis, FTI did a complete backup of the entire contents of each employee's mailbox, including deleted folders and other user-created folders. However, these backup tapes were not searched when responding to Shaw's subpoena. At the close of discovery, Shaw filed a motion for sanctions seeking to, in the alternative, dismiss GenOn's complaint, preclude FTI from offering expert testimony at trial and/or give an adverse inference jury instruction.

After Shaw filed its motion, FTI sought to restore 20 monthly backup tapes in order to retrieve any relevant email communications. FTI successfully restored 14 backup tapes, but was unable to restore six backup tapes. FTI produced to Shaw 46 additional emails from the 14 backup tapes it restored that were not included in its prior production. The court examined the circumstances surrounding these missing emails and determined that sanctions against FTI were unwarranted.

The first question before the court was whether GenOn had breached its duty to preserve evidence. Shaw contended that the data held by FTI was within GenOn's "possession, custody or control." The court determined that FTI had a duty to preserve evidence that pre-dated the issuance of the subpoena. The court examined both GenOn's legal and practical control of FTI's audit-related data. With respect to a legal right to FTI's audit-related data, the court could find no provision in the parties' retention agreement establishing that FTI had an affirmative duty to produce on demand its audit materials to GenOn. However, based on the relationship between GenOn and FTI, the court determined that GenOn had the practical ability to control audit-related data within FTI's possession. The court found, "[i]n light of FTI's continuing relationship with GenOn, and its role as a litigation consultant, there seems to be little doubt that FTI would have complied with a timely request by GenOn to preserve its information." Based on that determination, the court held that once GenOn determined that there was a reasonable likelihood of litigation with Shaw, GenOn had a duty to ensure that FTI preserved its audit-related data. The court next had to consider whether the missing emails pulled from the backup tapes suggested that Shaw was prejudiced by FTI's inability to pull data from the other six backup tapes.

With respect to the backup tapes as a whole, the court noted, "[w]hile the automated backup process consequently is not perfect, the primary purpose of backing up FTI's data is, of course, to facilitate business continuity and disaster recovery, not to ensure that the data is preserved for litigation. Given these business purposes, FTI did not require that its backup process have zero defects." In looking at the nature of the missing emails that were recovered from 14 of the 20 backup tapes, the court concluded that it was unlikely that any substantive discussions concerning the audit were lost due to FTI's inability to restore the data from those six backup tapes. Shaw's motion for sanctions was denied.

The *GenOn* case illustrates an important e-discovery principle. When a litigant determines that its duty to preserve has been triggered, it must consider whether potentially relevant electronic data is in the hands of any third parties. If so, the litigant needs to assess its legal ability to obtain that data from those third parties. The legal ability may arise by reason of agreement or statute. In some jurisdictions, including the Sixth Circuit, practical ability to control third party data must also be considered. Practical ability, as *GenOn* points out, will depend largely on the nature of the relationship between the litigant and the third party. Where the nature of the relationship evidences an ability to influence the third party to comply with requests for data, practical control is established. If legal or practical control over the data exists, the litigant then needs to include the third party in its litigation hold process. Had GenOn complied with its duty to preserve, FTI's faulty backup system probably would never have been exposed, and GenOn could have avoided the expense and risk associated with defending against Shaw's motion for sanctions.

- **B. Jay Yelton III** +1.269.383.5819
- **Kenneth J. Treece** +1.269.393.5810

FOIA Requests for Electronic Records

Freedom of Information Act coordinators have a difficult task nowadays given the exponential growth of electronic records. In order to ease the burden of responding to myriad requests for public records, FOIA coordinators should consider using the following practices used in civil litigation, which also must deal with large volumes of electronic records.

NEGOTIATE WITH THE REQUESTER

Oftentimes, a FOIA request is broadly written making compliance difficult, if not impossible. In such cases, the FOIA coordinator should negotiate with the requester about

- The time frame covered by the request. Seek to narrow when possible.
- The number of record holders. If lengthy, try to pare down to "key players."
- Search terms. Work to develop a list targeting the most likely responsive documents.
- De-duplicate the data. Agree that multiple copies of the same record do not need to be produced.
- Produce records over time. Agree that responsive records will be produced in stages beginning with the most highly relevant records.

USE SPECIALLY DESIGNED SOFTWARE TOOLS

These negotiating strategies make the most sense when combined with the use of special software designed specifically to locate and collect responsive electronic records. Once the potentially responsive records are found, the software can be used to reduce the volume by applying the negotiated time frame restrictions and search terms, and then de-duplicating the records.

When these steps are complete, the electronic records still need to be reviewed prior to production. Again, special software is available to process the records for viewing. The records are stored in a database and the software allows the user to mark the records that should be produced, those that are statutorily exempt from production, and those that contain some exempt information, but can be produced in a redacted format. Even notes regarding each record's treatment can be saved for later reference. These tools make keeping track of what decisions were made with respect to each record much easier. The information is stored in the database along with the records. So, if questions arise later with respect to a particular document, the FOIA coordinator can quickly locate the record and see what decisions were made with respect to that document.

CONCLUSION

In this age of electronic information, FOIA requests present the same challenges as requests for production of documents in civil litigation. FOIA coordinators should consider using the same strategies and software tools used in civil matters to make production of electronic information more manageable.

The authors will present an in-depth look at this topic in the Fall 2012 SRR Journal.

- **Kenneth J. Treece** +1.269.383.5810
- **Scott T. Wrobel,** *Stout Risius Ross* +1.248.432.1238