

DISCOVERY ISSUES IN
PATENT LITIGATION

Jeffrey C. Morgan
Christina Bost Seaton

Troutman Sanders LLP

The views and opinions expressed in this article are those of the authors and not necessarily those of Troutman Sanders LLP or its clients.

© 2008 Jeffrey C. Morgan and Christina Bost Seaton

All rights reserved

BIOGRAPHICAL INFORMATION

JEFFREY C. MORGAN

Jeff Morgan is a partner in the Atlanta office of Troutman Sanders LLP, where he specializes in Patent litigation. Jeff is co-chair of the American Bar Association's Trial and Appellate Rules Committee for the Intellectual Property Law Section.

Jeff has extensive experience litigating patent cases. He has represented a wide range of clients, from closely-held corporations to Fortune 500 companies, and in a wide range of technologies, including computer software, medical devices, industrial manufacturing machinery, lasers, and processes for manufacturing semiconductor chips.

Jeff received his J.D. from Boston College Law School, where he was an editor for the Boston College Law Review. He is a Fellow of the American Bar Foundation.

CHRISTINA BOST SEATON

Christina Bost Seaton is an associate in the New York office of Troutman Sanders LLP, where she focuses on commercial litigation, particularly issues pertaining to electronic discovery.

Christina received her J.D. from New York University.

DISCOVERY IN PATENT LITIGATION IN GENERAL

Vast amounts of electronically stored information (ESI), including emails, Microsoft Offices files (Word, PowerPoint, Excel, etc.), Voice-mail, Instant Messages, Databases, and deleted files, is stored on a wide array of devices, including, but not limited to, cell phones, PDAs, iPods, portable USB “thumb” drives, online storage, memory cards, and external hard drives. Managing this information is a complicated task in any litigation. The complexity of patent litigation, however, poses special challenges.

In patent litigation, the sheer volume of ESI can be enormous. It is not uncommon for some cases to initially identify over a terabyte of potentially responsive data. Not all parties in patent litigation are created equal, however, including when it comes to the volume of potentially responsive ESI. Counsel should always be aware of any such disparity. This is particularly true where small and large competitors are adverse to each other, or in situations where a non-practicing entity (for instance, a shell company holding rights to intellectual property) is adverse to a commercial entity. Small companies and non-practicing entities frequently have only a modest amount of ESI, in contrast to major companies which can have vast amounts of ESI.

Before any collective or production of documents begins, counsel for all parties should strive to agree upon the scope and volume of discovery. Some considerations include whether collection should be made from only centralized servers, or whether, under the circumstances of that case, collection should occur company-wide. Counsel should also think about from whom they should collect documents. It is important to determine upfront whether collection from only “key” custodians, as identified with help from the client, will be sufficient. Depending on the circumstances, the case may require that collection to occur company-wide, rather than being limited to “key” custodians. Keep in mind that these days, searches and collection of email are almost always required.

In situations where you seek discovery from a non-party, it is even more imperative that counsel work to limit the scope and volume of requested discovery. Keep the requested discovery simple and narrow. Counsel should not request from a non-party more information than they actually need to prove or defend their case. Non-parties view discovery as a burden in litigations in which they have no vested interest. Counsel should work with the non-party to address its concerns during the discovery process.

Similarly, when negotiating a protective order, counsel should ensure that the protective order covers material that will be produced by non-parties.

DRAFTING EFFECTIVE MULTI-TIERED PROTECTIVE ORDERS— FRCP 26(c)

When drafting and negotiating a protective order, it is important to first be knowledgeable about your client’s business, your client’s documents, and your adversary’s business and employees. When meeting with your client, you should ask such questions as:

- What types of sensitive documents does your client have?
- What harm would your client suffer if the adversary’s business people had access to those documents?
- Who are the types of individuals in your adversary’s business about whom you need to be particularly careful?

Armed with that and other similar information, you will be better equipped to determine what levels of confidentiality you will need to provide for in the protective order. For particularly sensitive documents, for instance, you will probably want to be able to designate them as Attorneys’ Eyes Only (AEO) rather than simply designating them as “confidential.”

In patent cases, multi-tiered layers of confidentiality protection have become the norm. There may be some documents, for instance, which would be especially damaging to your client were engineers from your client’s adversary to have access to those documents. You therefore might want to have one level of confidentiality for documents which could be viewed by your adversary’s business and technical employees, and another, higher level of confidentiality for documents that should be disclosed only to your adversary’s outside trial counsel and their experts.

Confidentiality in patent cases is further complicated by the special problem of source code. For many clients, source code represents millions (if not billions) of dollars of investment. If your client’s adversaries (or the public) were to obtain access to this source code, the client could suffer devastating effects on its business, potentially losing control of its intellectual property and of any competitive edge obtained through developing innovative code. In addition, like all ESI, the large volume of source code poses problems. Source code can be difficult to search without hierarchy or revision history software.

Because of the difficulties posed by source code, if source code is an issue in your case, you may want to seek additional protections for the source code in your protective order. One option is to provide that source code may be produced to the adversary only for purposes of inspection and only at your own office. Another option is using an escrow agent or Virtual Private Network (VPN) as a means of producing source code.

PROPER DESIGNATION OF DOCUMENTS

Once the levels of confidentiality in the protective order have been resolved (either by agreement with opposing counsel or through Court order), you will need to set up a system for classifying documents pursuant to that order. In close consultation with your client, identify which categories of documents are not confidential, which are confidential such that they should be shielded from the general public, which should be shielded from business people within your client's adversary's business, and which should only be shared with outside trial counsel and their experts.

As is often the case with discovery in complex cases, you may need to enlist the aid of a small army of document reviewers. If you do, you will need to effectively communicate to them what types of documents fall under which tiers of protection. Further, as they review and designate documents, you should continually monitor their work—taking steps to ensure that their designations are appropriate, accurate, and consistent. It can be embarrassing to find out later that a near identical document was classified under one level of confidentiality by one reviewer, but under another level by another reviewer.

MANAGING E-DISCOVERY

Preservation

Upon becoming aware of a claim against your client (or, if you are representing the plaintiff, upon becoming aware of a claim your client wishes to assert against others), you must work with your client to issue a litigation hold to preserve potentially discoverable data. In doing so, you should have detailed and frequent discussions with your client's IT director to identify the location of responsive ESI, and to suspend or modify any existing document retention/destruction policies.

The duty to preserve ESI arises “when the party has notice that the evidence is relevant to litigation or when a party should have

known that the evidence may be relevant to future litigation.” Zubulake IV, 220 F.R.D. 212, 216-17 (S.D.N.Y. 2003). There are many repercussions if electronic information is not properly preserved. For example:

- Zubulake V, 217 F.R.D. 309 (S.D.N.Y. 2003). Counsel must affirmatively monitor compliance with litigation holds and preservation letters.
- Phoenix Four, 2006 WL 1409413 (S.D.N.Y. May 23, 2006). Both defendant and outside counsel ordered to reimburse plaintiff for defendant’s failure to preserve evidence, including costs and fees for the spoliation motion and \$10,000 for each deposition that was re-taken by the plaintiff.
- United States v., Philip Morris, Inc., 327 F. Supp. 2d 21 (D. D.C. 2004). Defendant fined \$2.7 million because it destroyed potentially discoverable emails two years after the preservation order was entered. Defendant was also barred from presenting witnesses at trial who had failed to preserve relevant records.
- Coleman Holdings, Inc. v. Morgan Stanley & Co., 2005 WL 679071 (D. Fla. 2005). Defendant found to have overwritten emails, submitted false discovery certifications and failed to produce discovery. Court instructed jury that it could draw an adverse inference regarding the defendant’s malice or evil intent. Jury awarded \$1.5 billion in damages, of which \$850 million were punitive damages.

In order to ensure that you meet your preservation obligations, it is imperative to meet with the client’s business people and the client’s IT director as soon as possible. Together, you must work to identify where relevant ESI exists in the client’s systems, and to implement procedures to reduce the risk of inadvertent destruction of potentially relevant ESI. You should strongly consider enlisting the aid of a professional e-discovery preservation/collection vendor. Having a knowledgeable vendor involved from the beginning acts as a reality-check on your preservation procedure as the vendor is likely to have more experience across a wider variety of cases. In addition, the vendor can document, and if necessary, testify as to the reasonableness and thoroughness of the preservation efforts. See Peskoff v. Faber, 240 F.R.D. (D.D.C. 2007) (court ordered defendant to explain its search efforts used to locate discovery, and issued order

outlining the parameters of search for ESI when the defendant's search efforts were found to be lacking).

Collection (Search & Retrieval)

The large volume of information produced by most companies makes a purely manual search not feasible. Instead, an attorney's challenge is to choose the best search and retrieval method for the task. You must develop a collection plan arising out of your meetings with the client and with the preservation/collection vendor. If possible, you should meet and confer with opposing counsel in order to obtain agreement on the scope of discovery. Keyword searches work best when looking for specific phrases that are likely to yield relevant and responsive documents, but also make sure to include likely synonyms and misspellings to reduce the risk that other relevant and responsive documents are not overlooked. In addition, new conceptual-searching technology is beginning to appear with some litigation support vendors. Good de-duping software can also significantly reduce the time required for review.

Throughout the collection process, you should document when, where, and from whom all ESI/documents were collected. Also consider documenting why ESI/documents were NOT collected from a given source. This information could be valuable for your clients' (and your own) protection should there ever be any dispute as to your collection methods.

In any event, it is imperative that you do not open or view media that is not write-protected; take custody of the client's ESI without considering the chain of custody; review .pst files (emails) in Outlook (or any other type of emails in their native format); or print electronic documents. Doing so can lead to a loss of metadata for which your client can be held liable.

Review

When conducting your ESI document review, it is important to choose an appropriate review method/tool. Less sophisticated or more routine reviews may be able to be done in-house. In some circumstances, however, it may be worth exploring outside vendors' resources. If you are dealing with a large volume of ESI documents, you should also consider the pros and cons of hiring temporary attorneys to assist you with the document review.

Before the review, establish a document review protocol addressing which documents will be reviewed first and by whom. It may make sense to initially conduct a high-level review for only responsiveness and privilege. Later, you and your team can conduct a more detailed review for specific issues and key witnesses. Regardless, you should implement a clear and defined quality control procedure. For example, if you have decided to employ temporary attorneys for an initial, high-level review, you may want to have other lawyers in your firm do a quality check of a sampling of those reviewed documents (e.g., every tenth document) to make sure the documents are being properly classified. In any event, you should strive to quickly identify and address any unexpected issues as soon as possible.

Production

In which format should the documents be produced? Native? TIFF? PDF? Does that format contain metadata? What about using hashing? ESI presents a wide variety of issues that must be addressed during production that did not exist in the days of paper productions. The format of production is one of the topics the parties should discuss in the Rule 26(f) conference. Further, parties have an opportunity under Rule 34 to specify (or object, as the case may be) to the format of ESI production.

When choosing a format for production, keep in mind that native format may be useful, for instance, when you need to show how a program works, but producing in native format does not prevent against altering the documents by the reviewing law firm or experts. Further, it is extremely difficult to control documents produced in native form because they cannot be bates numbered. Some of that difficulty can be obviated by producing native files along with a “hash value.” Hash values are unique computer generated values that can accompany a native file production. Hash values, however, are not as easy to work with as bates numbered documents because they are not generated sequentially from document to document, but rather are the result of an algorithm performed on each individual document. As a result, they may be good to help establish authenticity and absence of tampering, but difficult to use in locating a document amidst hundreds of thousands of other documents.

Producing documents in TIFF or PDF format enable to you “lock down” the documents so they cannot be altered, and also permit you to control them by burning bates numbers on them. But TIFF and

PDF documents are more expensive to produce than native files, and they also do not always accurately reproduce certain files—most notably Excel spreadsheets.

Both types of production (native on the one hand, TIFF and PDF on the other) preserve metadata to varying degrees. Metadata is “data about data.” There are two common kinds of metadata, system metadata and application metadata. System metadata includes such things as the file’s name, location, format, and dates of creation, modification. It is generated automatically by computer. Application metadata, includes, for example, in Excel or other spreadsheet programs, the formulas underlying the data, or in word-processing programs, the comments or redlining within the document. Application metadata is created by people.

Other issues to consider include whether the documents produced may be read by OCR, a technology which makes searching within documents easier. ESI documents can be produced accompanied with an OCR text extract. Hard copy documents can be scanned and OCR text can be generated from that scan. Most document productions consist of OCR data to some extent.

It goes without saying that you should promptly review what you receive during production from your adversary. Doing so promptly permits you to address any perceived deficiencies as soon as possible. Throughout the process, document your efforts to meet and confer to resolve disputes. If it is not possible to resolve a discovery dispute with your adversary, you should promptly move to compel production of the relevant withheld information.

Admissibility

The parties should always work together and stipulate as to authentication and admissibility, including decisions to not assert or to waive objections such as hearsay. When the parties cannot do so, ESI presents difficult questions with regards to authentication. In *Lorraine v. Markel Amer. Ins. Co.*, 241 F.R.D. 534, 538 (D. Md. 2007), Judge Grimm set forth a useful test for the authentication of ESI:

- (1) Is the evidence Relevant—FRE 401
- (2) If Relevant, is it Authentic—FRE 901
- (3) If Authentic, if the evidence offered for its substantive truth or for some other reason?
 - (a) If not for substantive truth, it is “Not Hearsay”

- (b) If offered for substantive truth, it is hearsay and not admissible unless it falls into a hearsay exception—FRE 801
- (4) Is this the best evidence—FRE 1001-1008?
- (5) Does the probative value of the evidence outweigh the prejudice—FRE 403?

The *Lorraine* test provides useful guidance to attorneys who are seeking to admit electronic evidence at trial.

Authenticating ESI is especially difficult because of informality of many forms of ESI and fact that documents are often accessible to many people. Showing the reliability of the system used to create and preserve the document is therefore very important. Some of the admissibility considerations for specific types of ESI are:

- Email—may be insecure or unreliable
 - (a) FRE 901(b)(1)—person with personal knowledge
 - (b) FRE 901(b)(3)—expert testimony/comparison
 - (c) FRE 901(b)(4)—distinctive characteristics
 - (d) FRE 902(7)—trade inscription
 - (e) FRE 902(11)—self-authentication of business record by Declaration
 - (i) made by someone with “sufficient knowledge of the record-keeping system and the creation of the contested record to establish their trustworthiness”
 - (ii) document must have been created at or near the time of the matters recorded within the document
 - (iii) document must have been made by someone with personal knowledge of the matters recorded within the document
 - (iv) document must be made and kept as part of the regular course of business—“mere presence” in the business’ files not enough
 - (v) document was created by the employee at the direction of the employer
- Website Postings—information was likely posted by the host of the webpage

- (a) FRE 901(b)(1)—person with personal knowledge
- (b) FRE 901(b)(3)—expert testimony/comparison
- (c) FRE 901(b)(4)—distinctive characteristics
- (d) FRE 901(b)(7)—public records
- (e) FRE 901(b)(9)—system or process producing a reliable result
- (f) FRE 902(5)—official publication
- Text Messaging—informal communication
 - (a) FRE 901(b)(1)—person with personal knowledge
 - (b) FRE 901(b)(4)—distinctive characteristics
- Chat Room Content—difficult because posted by people other than the website host
 - (a) FRE 901(b)(1)—person with personal knowledge
 - (b) FRE 901(b)(4)—distinctive characteristics
- Computer-Stored Records/Databases—show process used to preserve record so fact-finder feels comfortable that record that is being admitted is the same record that was originally created
 - (a) FRE 901(b)(1) person with personal knowledge
 - (b) FRE 901(b)(3) expert testimony/comparison
 - (c) FRE 901(b)(4)—distinctive characteristics
 - (d) FRE 901(b)(9)—system or process producing a reliable result

In *In re Vee Vinhnee*, 336 B.R. 437 (9th Cir. 2005), the Ninth Circuit adopted the eleven-step evidentiary foundation proposed by Professor Edward Imwinkelreid for the authentication of electronic business records:

- Business Uses A Computer
- Computer Is Reliable
- Business Has A Procedure For Inserting Data Into Computer
- Procedure Has Built-In Safeguards To Ensure Accuracy And Identify Errors
- Business Keeps Computer In Good State Of Repair

- Witness Made Computer Read Out Data
- Witness Used Proper Procedure to Produce Read Out
- Computer Was In Working Order When Witness Obtained The Read Out
- Witness Recognizes Exhibit As The Read Out
- Witness Explains How He Recognizes The Read Out
- If Read Out Has Unusual Symbols, Witness Explains Symbols To Fact Finder

336 B.R. at 446-47.

RECENTLY AMENDED FEDERAL RULES OF CIVIL PROCEDURE REGARDING ESI

On December 1, 2007, new amendments to the Federal Rules of Civil Procedure went into effect, many of which address the obligation to preserve, collect, and produce ESI.

- a) FRCP 26(a)(1)—Your mandatory initial disclosures now must include a copy or description by category of ESI.
- b) FRCP 26(f)—Meet and Confer—at the discovery planning conference, counsel must be knowledgeable and familiar with their client’s ESI. You should consider how discovery relates to non-parties, determine whether metadata and ESI should be produced; consider ways to balance your clients’ competing needs of preserving relevant evidence and continuing with routine business operations. You should also determine agreeable protocols (such as “quick peek” and “clawback” agreements) that minimize the risk of privilege waivers and reduce costs and delays of production.
- c) FRCP 16(b)—Scheduling Order—after receiving the Rule 26(f) report from the parties, or after a scheduling conference, the district judge will enter a scheduling order that may:
 - “...(3)(B)(iii) provide for disclosure or discovery of electronically stored information; (iv) include any agreements the parties reach for asserting claims of privilege or of protection as trial-preparation material after information is produced.”
- d) FRCP 34(b)—the request for production may specify the form or forms in which ESI is to be produced. Responding parties may

object to the requested form and propose an alternative form of production.

- e) FRCP 37(e)—Very Limited “Safe Harbor”—this rule adopts a “good faith” standard of culpability for the imposition of discovery sanctions when information is lost due to “routine” operation of an ESI system. “Routine” means the “ways in which such systems are generally designed, programmed, and implemented to meet the party’s technical and business needs,” while “good faith” is measured by the steps that the party took to preserve ESI and to stop the destruction or loss of information by the “routine” operation of an electronic information system. Your client must have a “reasonable and consistently-enforced” document retention policy. See FRCP 37 Advisory Committee Notes (2006). Nonetheless, that policy should be suspended for a sufficient time to adequately preserve discoverable ESI.

Note that even when the Safe Harbor applies, it does NOT prevent courts from ordering relief OTHER than sanctions.

Qualcomm - A Cautionary Tale

The penalty for failing to preserve, collect, and produce responsive ESI can be severe. In *Qualcomm Inc. v. Broadcom Corp.*, 539 F. Supp. 2d 1214 (S.D. Cal. 2007) the Court imposed heavy sanctions on Qualcomm for its failure to produce relevant e-mails and other ESI. Near the end of trial, Broadcom’s attorney was cross-examining a Qualcomm witness. That witness indicated that she was aware of several emails which related directly to the key issue at trial. Those e-mails had not been produced, however. It was later determined that approximately 200,000 pages of e-mails, memoranda, and other responsive ESI had not been produced. The court determined that the Qualcomm’s attorneys had engaged in “an organized program of litigation misconduct” and the Court invalidated Qualcomm’s patents. The court ordered that Qualcomm pay Broadcom’s legal fees, which were over \$10 million, and it individually sanctioned plaintiff’s attorneys, including the associate and junior associate, who had, at that time, brought up the discovery issue to their supervisors. Qualcomm was found not to have conducted basic searches that would have found the unproduced emails, and Qualcomm’s counsel was faulted for taking the word of its client that those e-mails did not exist.

The *Qualcomm* case is currently being appealed, but it illustrates a potential nightmare scenario of electronic discovery gone awry. Protect yourself and protect your clients by being vigilant about preserving electronic evidence, keeping good notes of your discovery policies and procedures, and by producing responsive documents.

NOTES

NOTES