

Controlling E-Discovery Costs in IP Matters— Are You Being Penny Wise and Pound Foolish?

By Richard Finkelman and David A. Gustafson

IP matters have many unique elements requiring planning and thoughtful decisions by the legal team. Some events, a *Markman* hearing for example, are easy events to point at and agree that important decisions need to be made. Other, less obvious, examples involve locating and preserving potentially responsive electronically stored information (ESI) early. As the legal team involved in the Qualcomm matter learned, not locating responsive ESI can be disastrous. While the risks of e-discovery become obvious when thousands of e-mails are produced at trial, the risk-reward decisions made in the very beginning of a matter are not always so obvious.

Recent research commissioned by McAfee, Inc., indicates that the current global recession is presenting additional risks to the protection of intellectual property from the standpoint of data protection and security/access breach prevention.¹ While the focus of this particular research implicates reductions made in expenditures on data security and associated support resources as a major area of risk and concern for organizations involved in the creation of and profit from intellectual property, the common thread is that organizations are actively seeking means to reduce costs associated with IP protection, including costs associated with litigation and e-discovery associated with such protection. This article addresses some of the most common costs associated with e-discovery and helps you ask and answer the question, are you being penny wise and pound foolish in your IP practices relating to e-discovery.

More specifically, this article focuses on components of the e-discovery process generally at play in a legal matter involving the protection of rights and ownership of an organization's IP assets. It also focuses on practical ways of containing these costs in an enterprise landscape of budget and staff reductions, a bewildering and often overwhelming array of new rules, multiple venues, overwhelming volumes of electronic discovery materials, and a prevailing opinion of e-discovery as a "morass."²

Example Scenario

To set the stage for this discussion, the following thumbnail sketch of a hypothetical situation addresses the intersection with discovery concepts and highlights the areas where cost

Richard Finkelman is a managing director and the practice leader of the Discovery Services practice at Navigant Consulting. **David A. Gustafson** is a director in the Discovery Services practice of Navigant Consulting, where he specializes in consulting with organizations responding to discovery requests and in formulating information management strategies to mitigate costs and risks associated with these efforts. Mr. Finkelman can be reached at RFinkelman@NavigantConsulting.com or at 949-660-8244. Mr. Gustafson can be reached at DGustafson@NavigantConsulting.com or at 646-227-4355.

containment might be achieved without introducing unacceptable risk. Company X is named as a defendant in a matter alleging that the company has improperly integrated third-party-patented technology in one of its products. Most patent cases involve some common discovery elements including ESI about the accused technology in the company's products and in potential derivative products. Other ESI commonly sought includes sales and other accounting records, as well as document repositories and, often, Internet and intranet data about the products at issue.

For purposes of brevity, we shall omit discussion of the preliminary legal steps the defendant company and its counsel would pursue in defending these allegations and move directly into discussion of the relevant aspects of the discovery process that present themselves as areas where prudent decision making and use of available discovery techniques and technology can simultaneously reduce associated risks and costs.

An oft-cited model for the discovery life cycle in a litigation matter is the Socha-Gelbmann EDRM reference model.³ Depicted below in its familiar form, this model serves as a useful means of isolating aspects of the discovery process for analysis of associated risks and costs.

Each of the individual boxes depicted in the model refers to a set of processes, activities, or requirements associated with the discovery life cycle. We will start our analysis with the box titled "Information Management" and with a focus on the phases appearing to the left of the Processing/Review/Analysis phases to analyze the cost components potentially relevant in our hypothetical scenario presented above and means by which these costs might be mitigated. While some discussion is afforded to the latter phases of the discovery life cycle, the "downstream" costs typically associated with e-discovery are largely a function of the thought and work conducted upstream. In other words, by carefully orchestrating the initial scope and approach to discovery response efforts, counsel and their clients can both mitigate risks presented by evolving rules and legal precedents dealing with e-discovery and control runaway costs often encountered when each phase is coordinated and executed in a vacuum without a cohesive discovery response strategy or set of methodologies in place.

To this last point, and as a guidepost for any subsequent recommendations appearing in this piece, counsel and their clients are strongly urged to enlist the assistance of internal or external resources with discovery expertise, experience, and appreciation of the full discovery life cycle, rather than those whose knowledge lies only in specific parts of it (e.g., document collection, processing, review, etc.) For instance, relying on guidance regarding practical *and* prudent means to safely define and limit preservation requirements from

experts from an organization that specializes in processing data—generally a price/volume driven endeavor—may not engender the type of advice that has the total cost of discovery response efforts in mind. Further, it should also be noted that relying solely on the advice and direction of discovery experts without the full and active participation of legal counsel and relevant stakeholders from the client organization may expose parties to undue risk due to lack of fluency with relevant legal issues, precedents, or strategy. A cohesive discovery response strategy that is capable of simultaneously mitigating risk and controlling cost must consist of representatives who bring legal, technical, risk management, and solid project management skills to a common table.

Information Management

This phase of the discovery life cycle really deals with getting the lay of the land within the organization—Company X in our example—so as to understand what potential repositories may contain ESI for the matter at hand. Many organizations have taken the proactive measure of generating an “inventory” or “data map” of their repositories of ESI. Creation of a data map or inventory may be part of a broader litigation or discovery-readiness initiative within an organization or may occur as part of initial efforts in response to an anticipated litigation matter.

These maps may include details about the type of data contained within the specific repository (e.g., e-mail, documents, financial/transactional data, etc.); who the relevant business and/or technical support “owners” of these systems are with relevant contact information; the relevant retention period imposed on the data contained within the repository; information about backup and archival policies and practices for these systems; and perhaps also some comment about the steps necessary to collect or extract data or documents from these repositories. Referring back to our hypothetical scenario, a data map for Company X might also contain information

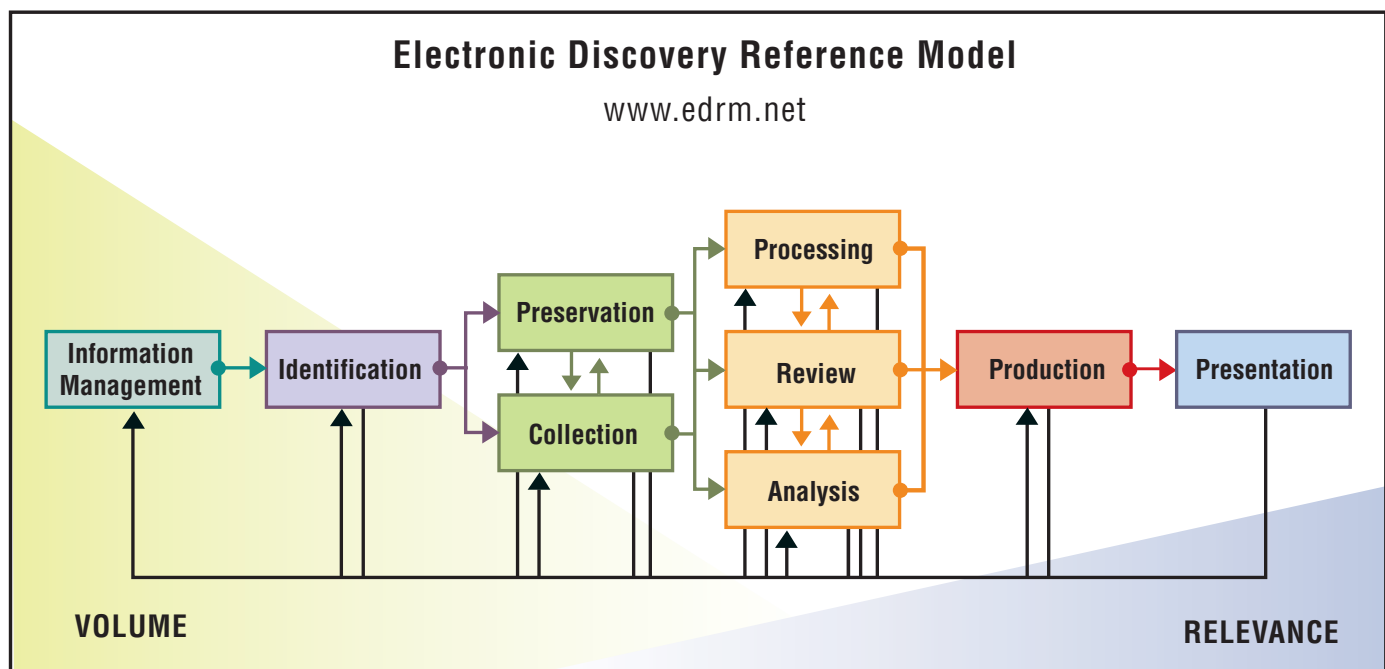
about repositories of programming language (code library), development documentation, or underlying enterprise applications for house accounting and sales information.

Direct benefits of a well-maintained and comprehensive ESI inventory include the ability to more efficiently and accurately prepare required Rule 26(a) discovery disclosures and respond to any overly broad discovery requests initially received or put forth during subsequent Rule 26(f) conferences. Starting with a spreadsheet is one of the best ways to figure out where potential ESI might be. The spreadsheet should include the complaints or allegations in a column, with other columns for products, ESI types and locations, and effort required to preserve. The below illustrates what a sample spreadsheet might look like.

Once completed and coupled with a data map or other list of ESI locations, responding parties have greater agility in responding to and narrowing the effective scope of such requests, thus reducing the subsequent downstream volume of documents and data that ultimately require processing, review, and production. Absent the availability of this type of inventory, the initial process of responding to a discovery request can be truly daunting. The responding organization must scramble to identify the sources of potentially relevant materials. In the midst of responding to a crisis or interruption of an organization’s normal business activities due to the discovery requirements of an active or pending matter, the amount of time and resources that must be dedicated to thoughtfully preparing a response to an overly broad discovery request is frequently curtailed. The result is the preservation, collection, processing, review, and production activities involving mountainous volumes of irrelevant and/or unresponsive materials.

Identification

The identification phase is frequently the most pivotal phase of a discovery effort, as the scope, scale, and methodology of efforts to identify potentially relevant materials will have a



direct impact on the overall discovery costs. This is the phase where parties will gain an initial understanding of the volume of data/documents involved and the complexities inherent in each subpopulation of materials that may require special handling or analysis. This identification phase involves the identification of not only repositories of potentially relevant ESI, but also custodians of potentially relevant ESI and/or individuals who are familiar with the issues and who require interviews or follow-up. The identification phase also leads directly into the preservation phase, which will be discussed in the next section, and which also has a direct impact on the overall costs of discovery.

Identification of potentially relevant custodians and repositories of ESI may require an iterative approach starting with the most basic understanding of the technical and legal issues at hand and continuing in a progressively deeper dive into the issues and relevant data and documents. It is important during this phase to thoroughly document the individuals contacted or interviewed, the information gathered during this due diligence, and the nature and logistics of the potentially relevant repositories of ESI mentioned during the fact-finding phase. Organizations frequently find it useful to make that

of the product or service from design to testing, implementation, and resulting sales and marketing efforts. As the scope of inquiry increases, the potentially relevant number and nature of ESI repositories may expand as well. For example, the type of system or repository utilized by an individual involved in the sales or marketing of the technology innovation are arguably different than those used by development personnel writing lines of programming code for key system functionality. Where possible, it is advisable to schedule the custodian and ESI source identification due diligence events soon and in close proximity to each other. Bundling interviews with cross-functional personnel may save time and expense as well, particularly when dealing with larger, more geographically distributed organizations.

Similarly, as is suggested in the hypothetical case scenario presented above, the nature of data or documentation relevant to a particular matter may require specialized resources to assist counsel with its interpretation or translation in order to establish relevance and/or responsiveness. In our example, subject matter experts may be required as potential ESI data are located and evaluated. Specific resource requirements for such analysis and interpretation should be identified and

Allegations	Product	ESI Type/Location	Preservation Effort
Product Z uses Accused Technology	Z and derivative products	E-Mail: Servers Doc Repository 1 Website 1, Intranet Sites 14, 25, 33	Easy Medium Hard
Product F uses Accused Technology	F; no derivative products	E-Mail: some on tape from acquisition and time period Doc Repository 2	Maybe hard Unknown

initial spreadsheet a living document. Additional columns can be added to track progress during this step and the ones that follow. This information may become relevant to subsequent efforts to establish and prove that adequate measures were taken to identify all relevant sources of ESI. It also serves the dual purpose of reducing the chance of duplicating effort and expense.

It bears repeating that the scope of due diligence required to determine relevant subject matter experts, custodians, and potentially relevant repositories is largely dependent on the nature of the matter at hand. For example, in our hypothetical scenario involving Company X, while the initial scope of inquiry and due diligence may begin with relevant technology development and business-line management personnel, this scope could easily expand to personnel involved in marketing, sales, or other functional areas within the organization that may have had something to do with the evolution

engaged as soon as the need appears necessary.

In cases involving alleged IP or trade secrets theft, it is frequently necessary to examine the workstation(s) and network computing locations utilized by personnel under investigation or of interest. This type of analysis, commonly referred to as forensic analysis, also requires specialized tools and personnel to determine whether evidence of malfeasance is present on various electronic media. If a matter involves allegations of theft or unauthorized access/transfer of electronically stored intellectual property or trade secrets, counsel should take immediate action to engage appropriately credentialed resources to assist in the analysis and processing of this type of data. Delay in identifying possible locations where such trespasses may have occurred can result in loss of potentially relevant evidence, culminating in unfavorable rulings or sanctions, or damage to the organizations' ability to pursue a specific course of defense or relief. While this article is

not intended to serve as a primer on computer forensics, the key point here is that ESI, unlike its paper predecessors, has ephemeral and volatile characteristics that dictate quick but careful consideration and response.

Preservation

As relevant custodians and sources of ESI are identified, parties are obligated to assure that data are not inadvertently destroyed or subject to normal retention periods. Taking necessary action on some ESI repositories can be extremely complex and/or prohibitively expensive, so it is critical to document the steps required to do so in the event it becomes necessary to argue undue burden to the court. For example, in many, if not all, financial services operations, there are several transactional systems that are designed for high-performance, high-volume transaction processing and are not designed to be preserved in the same way that e-mail or Microsoft Word or Excel files residing on a network file server might be preserved. If there are extenuating reasons why a particular repository cannot be adequately preserved to the satisfaction of all parties, counsel is advised to bring these to the attention of the court and all requesting parties soon rather than later so as to avoid an allegation that inadequate attention was paid to this requirement.

Mention was made in the prior section about the ephemeral nature of ESI, but another important characteristic of electronic data is its tendency to multiply—working copies are made, often in several locations; routine disaster recovery and/or retention practices are executed; documents are distributed via e-mail or migrated to common repositories such as shared network drives, collaborative worksites, and intranets. All of these locations must be considered when contemplating preservation requirements for a matter and as plans are drawn to move towards data collection.

As for preservation requirements for the more frequently encountered types of ESI (e.g., e-mail, word processing documents, spreadsheets, etc.), the duty to assure adequate preservation of these materials begins at the point at which there is reasonable expectation of litigation and extends through the course of the litigation or until there is a clear communication that specific subpopulations are no longer subject to preservation requirements. Again, given the volume and complexity of ESI in modern organizations, this requirement alone frequently presents challenging and expensive problems to responding parties, even before the subsequent phases of collection, processing, analysis, review, and production take place. However, this area is key; incomplete efforts can result in costly sanctions or requirements for work duplication.

Technology is available in the market to facilitate the communication of preservation notifications to affected custodians and to issue periodic reminder notices that are critical in matters spanning long periods of time. Whether the responding organization or its representative counsel invest in such technology or rely on more traditional means (e.g., e-mail notices), this is an important consideration in organizations where frequently those responsible for ongoing creation of ESI relevant to the matter may not be aware of their obligation to continue preservation throughout the course of

the matter. Attention must also be paid, not only to preserving materials initially identified as potentially relevant, but also to identifying and preserving any subsequent data or documentation that may be deemed relevant. Periodic and routine follow-up reminders and/or collection efforts should be designed to accommodate such scenarios.

Another major cost component associated with the preservation phase includes the means by which potentially relevant documents and data are preserved. It is frequently the case that potentially relevant materials are merely taken “out of commission” and out of the hands of those within an organization who must continue to use these materials to conduct its daily operations. This is unacceptable. Companies responding to discovery requests are frequently faced with the necessity of making copies of potentially relevant ESI on “preservation servers,” segregating e-mail accounts for potentially relevant custodians to separate e-mail servers and/or enabling “journaling” functions such as those in MS-Exchange, relying on e-mail archive solutions for extended retention of potentially relevant materials, or (blindly) relying on disaster recovery processes and technology as a backstop preservation approach. This latter approach, as parenthetically suggested, is fraught with risk and hidden costs.

Much has been made of the courts’ efforts to differentiate between reasonably “accessible” and “inaccessible” data. Disaster-recovery media (e.g., tapes) have been lumped with other materials in the “inaccessible” category. However, failure to preserve materials in the manner in which they are stored in the ordinary course of business may incur court sanctions and the obligation to perform costly restoration of materials from disaster recovery media. The effort can be painful at best, as anyone can attest who is familiar with recent headline-grabbing incidents involving backup tapes or unfortunate enough to have gone through the process themselves.

The prospect of maintaining preservation copies of volumes of potentially responsive discovery materials may represent an unanticipated cost; the repercussions and costs of failing to preserve evidentiary materials can easily render these burdens and costs relatively insignificant. Prudent planning and decision making further upstream to identify and isolate relevant sources of ESI can mitigate these unanticipated costs and spell the difference between an efficient, cost-conscious response and one that is reactionary, difficult to defend, or the cause of rulings unfavorable to the client.

Collection

Frequently concurrent with or shortly following preservation efforts, e-discovery activities often evolve into steps relating to the extraction of data from native ESI repositories for purposes of preservation and/or subsequent processing/analysis/review. As is the case with other aspects of the e-discovery life cycle, there is no real formula or one-size-fits-all approach to this phase. Methodology and technology deployed for these purposes are largely dependant on the nature of the documents and data involved in the matter. Collection methodology and resource requirements should be driven by the results of due diligence during the identification phase and may need to be supplemented as additional

material is identified or deemed potentially relevant.

Again, although this article is not intended to serve as a primer on electronic evidence or forensic collection methodologies, there are some basic principles at play that apply to these activities, regardless of the type of data or media involved. Borrowing from the medical profession and the oft-quoted Hippocratic Oath, the phrase “Above all, do no harm” seems an apt expression here. Regardless of the type of data or media involved, great care must be taken towards protecting the integrity of the evidentiary material, avoiding spoliation, and observing strict chain-of-custody procedures. Failure to observe basic principles in the handling of ESI can have costly repercussions. That said, readers are advised to seek the counsel of those experienced in the collection of electronic evidence from a wide range of potential sources.

While extraction/collection of materials from a computer hard drive, network share location, e-mail server, or collaborative work site may seem to be a commodity-level task best awarded to the lowest bidder, there is no substitute for experience and track record in this area, and particular emphasis in service procurement should be placed on checking references and experience levels of vendor candidates. Also, as previously discussed, specific types of ESI may require specialized approaches to collection of such matters as programming code, data residing in transactional systems, data residing in relational database systems, or other proprietary systems that may require uniquely qualified resources to successfully perform extraction or collection.

Often, due to efforts to minimize disruption to business operations or confidentiality concerns, collection efforts are limited to one opportunity. Going back to the well frequently is not an option; it is one that has unwanted negative consequences. Further, readers should familiarize themselves with the basic concepts behind some of the more frequently utilized tools for data collection in order to make informed decisions as to the most effective and efficient means to proceed. For instance, while performing a forensic acquisition of every piece of electronic media may be the most cautious approach and warranted in some situations, it is not necessarily the only way to preserve precious “metadata” associated with ESI and should be understood in terms of what additional steps (and costs) are associated with dealing with individual documents or data sets that are captured using such methodologies and technology.

Taking a forensic gunslinger approach of “forensically capture everything” and letting the subsequent processing steps (keyword filtering, de-duplication, etc.) sort out the wheat from the chaff can be a time-consuming and expensive proposition. Understanding the capabilities of specific technology approaches and asking competing vendors for their insights as to what they consider to be “best practices” can reveal much in terms of what approaches are appropriate in specific instances.

Processing/Review/Analysis/Production/Presentation

As potentially relevant ESI is identified, preserved, and collected, it is generally staged for additional handling prior to making a final determination about its evidentiary value. ESI and data are filtered to identify materials responsive to specific criteria (date, keyword responsiveness, etc.), duplicates are removed, and resulting materials are loaded to one or more repositories for subsequent evaluation for relevance, privilege classification, or other purposes.

The vendor and technology choices available for processing and repository services are seemingly endless, each with its own set of advantages, costs, and risks. While these are outside the intended scope of this article, readers are reminded that, as is the case with collection methodologies, there is no real one-size-fits-all solution here and the most optimal solution for one set or type of ESI may not be the same solution for another.

For example, there are several products on the market today that make use of “conceptual or thematic” clustering to facilitate more efficient review of similarly themed documents. These solutions offer great promise of efficiency where there is a high proportion of e-mail and electronic “office” documents such as letters, memos, spreadsheets, and presentations that are of little or no value in circumstances where the bulk of potentially relevant evidence lies in relational databases, programming code, or graphic files such as digital photographs, sound files, or movies. The guidepost here is to let the results of your due diligence drive the processing, review, and production technology approach decisions, rather than the opposite.

Conclusion

The focus of this article has been on e-discovery phases that are generally considered to be “upstream” from those involving the processing, analysis, review, and production of evidentiary material. Not to diminish the significance of these important phases or to suggest that each downstream phase does not contain its own set of cost and risk considerations, but it is important to note that the initial scope-setting phases associated with the e-discovery life cycle are frequently overlooked or underserved despite their potentially significant, direct impact on the costs associated with “downstream” document/data processing, attorney review, and production. ■

Endnotes

1. MCAFFE ET AL, UNSECURED ECONOMIES: PROTECTING VITAL INFORMATION (2009), <http://resources.mcafee.com/content/NAUnsecuredEconomiesReport>.
2. INTERIM REPORT ON THE JOINT PROJECT OF THE AMERICAN COLLEGE OF TRIAL LAWYERS TASK FORCE ON DISCOVERY AND THE INSTITUTE FOR THE ADVANCEMENT OF THE AMERICAN LEGAL SYSTEM, (Aug. 1, 2008), <http://www.actl.com/AM/Template.cfm?Section=Home&template=/CM/ContentDisplay.cfm&ContentID=3650>.
3. Socha-Gelbmann Electronic Discovery Reference Model, www.edrm.net, (last visited June 24, 2009).