Bloomberg BNA

Digital Discovery & e-Evidence®

CASE MANAGEMENT

Daniel K. Gelb and Richard M. Gelb explain how currently available technologies, when properly applied, can facilitate coordination among joint defendants in complex legal proceedings. They argue that savings in legal fees and costs resulting from efficiencies affords more insurance coverage for settlement and advocacy purposes.

Re-Defining the Role of eDiscovery Among Joint Defendants

By Daniel K. Gelb and Richard M. Gelb

Companies and/or their officers, directors and employees confronting complex and protracted legal proceedings—such as securities and financial fraud claims—must defend themselves against both derivative and class actions. Additionally, the nature of the claims often results in actions by federal and state regulatory agencies, including the United States Securities and Exchange Commission, and criminal prosecution by the United States Department of Justice.

Typically, the company under its bylaws is obligated to advance legal fees and provide indemnification. Even if directors and officers (D&O) insurance coverage is available, coverage is frequently inadequate.

Daniel K. Gelb and Richard M. Gelb are partners at the law firm of Gelb & Gelb LLP (www.gelbgelb.com) in Boston, Massachusetts where they represent clients facing complex commercial litigation, criminal prosecution, and regulatory proceedings.

Complex legal proceedings will almost invariably involve large volumes of electronically stored information (ESI)[1] captured from numerous custodians employed by an organization. It is not unusual for large corporations to spend hundreds of thousands—or even millions—of dollars in electronic discovery (eDiscovery) related expenses.

Although this might be the trend, it should not—and does not—have to be the fiscal benchmark by which litigation costs are measured. Litigation strategy is not to be divorced from budgeting discovery, which is why practitioners must leverage cost-effective approaches to eDiscovery—regardless of whether the volume of ESI at issue is 10 gigabytes or 10 terabytes.

Depending upon the case and relationships among the individual defendants (or targets) involved, many parties enter into joint defense/common interest agreements. However, although they have ''common interests,'' each defendant may have a different legal strategy. For example, the company CEO may seek to shift blame to his CFO, who in turn, will look to the Controller, and so on.

This dynamic is nothing new; however, the proliferation of ESI makes coordination among joint defendants more challenging, and as a result, cost control more imperative.

Proportionality, Coordination, and Forensics. eDiscovery must be cost-effective relative to the stakes and scope of the case. Conceptually, eDiscovery is more

[1] For convenience, the term ESI as used in this article includes both hardcopy and electronic files.

 ISSN 1941-3882

than merely capturing ESI for privilege review and document production. Rather eDiscovery practices can be strategically utilized to control—rather than increase—legal fees and costs.

As a threshold matter, in-house counsel must be conversant with the process required to properly preserve, collect, manage, review and ultimately produce ESI in order to effectively oversee ESI projects.

Presumably, outside counsel engaged to undertake an internal investigation will be independent, and therefore, may initially be unfamiliar with the company's information systems, IT schematics and data architecture. In-house counsel should work closely with outside counsel and the company's information technology personnel to formulate an appropriate, documented and legally defensible ESI protocol.

A forensics expert should be included as a team member so that reasonable efforts in handling ESI can be demonstrated and the required chain of custody for admission of ESI into evidence can be established in the event a given dispute places the capturing, chain of custody and review of certain data at issue.

Counsel must be conversant with the process required to properly preserve, collect, manage, review and ultimately produce ESI in order to effectively oversee ESI projects.

Hosting ESI for Use by Joint Defendants

Once captured and preserved, ESI should be culled, processed and subsequently hosted on a review platform. Document review tools need not be relegated to linear review. They can also provide an efficient method, specific to particular complex legal proceedings, for accessing ESI involving voluminous amounts of varying data types.

Particularly in regulatory proceedings, selecting a litigation support vendor involves an evaluation of, among other nuanced criteria, the level of encryption certification, and whether the hosting platform has support from an attorney on staff for purposes of quality control concerning, for example, documents with sensitive information (i.e. financial/bank statements, medical records and ESI generated by cross-border organizations governed by the EU Data Directive).

Regulatory Data Delivery Standards. Moreover, it is important that the eDiscovery vendor be familiar with the given data delivery standards for the regulatory authority to which documents and ESI may be produced. Notably, when responding to a subpoena in the context of a securities enforcement investigation, the United States Securities and Exchange Commission has its own *Data Delivery Standards*, available at (http://www.sec.gov/divisions/enforce/datadeliverystandards.pdf).

Practitioners must also be familiar with *Recommendations for Electronically Stored Information (ESI) Discovery Production in Federal Criminal Cases* developed by the Department of Justice/Administrative Office Joint Working Group on Electronic Technology (''JETWG'') available at (http://www.fd.org/navigation/litigation-support/subsections/esi-protocol-jetwg-recommendations-for-esi). The JETWG recommendations were developed for federal criminal proceedings.

Counsel should integrate both an understanding of the current rules of procedure and administrative trends relative to the management of ESI across governmental agencies into the overall eDiscovery management strategy for the joint defense team in order to achieve uniform approaches for handling ESI. This is especially important when parallel proceedings are reasonably anticipated.

Initial Strategic Decisions. Initial strategic decisions must be made not only about the volume and scope of review of the eDiscovery at issue, but also with respect to the logistical management of ESI and the manner in which targets and their counsel can access hosted information and comport to a joint defense agreement should one be in place.

First, the company should not divest control of ESI to the law firm engaged to undertake the internal investigation because doing so will give the company fewer options if it wishes to replace that firm in the future or use other firms for certain projects.

Second, *both* the company *and* joint defendants can use the same web-based document review tool so long as virtual partitions are integrated into the platform in order to prevent compromising the protections afforded by the attorney-client privilege and work product doctrine.

Third, there may be enhanced benefits for the company when cooperating with prosecutors and regulators if ESI is produced in an efficient and user-friendly manner.

Important Features of Review Platforms. Significantly—and often overlooked—certain features of a hosted document review platform become critically important when, for example, counsel represents a company's current CFO, and the Department of Justice is targeting a number of financial transactions. Counsel for the CFO may be concerned about the CFO's involvement in one of the transactions and wish to analyze the CFO's exposure. Counsel for the CFO must obtain the ESI necessary for an analysis from the company's outside counsel if that is where the ESI resides and is controlled. As a result, the issues concerning the CFO will appear on the radar screen.

However, counsel can analyze ESI hosted on a password-protected platform *sub rosa,* which protects the CFO by affording confidentiality.

Management of ESI Among Joint Defendants

Engaging Lit Support Personnel. Joint defendants should engage a common litigation support vendor independent from the target company to manage the ESI obtained from the company and exchanged among the joint defendants, even if the company itself were charged with hosting the documents.

Joint defendants working as a group can incorporate efficiencies with their legal counsel by using a single eDiscovery consultant. The consultant should be a signatory to the joint defense agreement, and the parties must all be explicitly clear about for whom the vendor

  DDEE ISSN 1941-3882

will provide services and the scope of such services, and how the attorney-client privilege and work product doctrine protection will be preserved.

Importantly, the litigation support vendor is separate from the vendor providing the review tool, and therefore, should become familiar with the features of the given software hosting platform and avail him or herself of ongoing support.

The support consultant will enable counsel to work more efficiently by coordinating review efforts among joint defendants.

This approach avoids the ''silo effect'' among numerous law firms party to the joint defense agreement.

In addition, leveraging eDiscovery consultants will substantially lessen the case's demand for attorney review, production and management time.

Finally, an efficient approach to eDiscovery and hosted review will avoid eroding the D&O coverage through unnecessary attorney time.

Benefits of Neutral Repositories. Second, to save attorney time, the litigation support consultant, with the assistance of counsel, can coordinate ESI searches across the joint defendants (e.g., there may be search terms pertinent to every joint defendant).

Third, the joint defendants can identify factual and legal issues common to all of them, and relevant ESI can be extracted and hosted by the common vendor on the common platform and remain equally accessible to all joint defendants. Since password protection will be enabled, the hosting platform becomes a neutral repository of ESI for which a target will not need to risk waiving a legal privilege when accessing and reviewing the hosted documents.

Once again, each joint defendant can retrieve information without compromising the protections of the attorney-client privilege and work product doctrine.

Educating Counsel for the Joint Defendants

Because many large-scale legal proceedings such as securities and financial fraud matters require the involvement of numerous attorneys, technology allowing users to conduct web-hosted seminars provides a valuable tool for educating counsel for the joint defendants, and obviating any concerns that the parties will be going in different directions with respect to their understanding of the pertinent legal issues and identification of documents relevant to those issues.

Leveraging eDiscovery consultants will substantially lessen the case's demand for attorney time.

Consider a scenario in which legal proceedings arise from the allegedly improper recognition of revenue published to the investing public through the company's financial statements.

Counsel for the joint defendants can engage one accounting expert to conduct in-person or web-based seminars for counsel in order to explain applicable accounting rules in a setting where communications and exchange of documents are protected by the attorney-client privilege and work product doctrine. This arrangement should be addressed in the joint defense/common interest agreement, with the caveat that the accounting expert is not permitted to provide consultation to individual joint defendants independently of the others.

Importantly, common knowledge enhances the mutual development of legal strategies, minimizes the risks of inconsistent legal positions and wasting the insurance coverage as result of inefficient lawyering.

Privileges. Communications among joint defendants and the common consulting expert are protected by the attorney-client privilege and work product doctrine. This facilitates use of the expert in formulating strategy, case evaluation, identifying key documents and preparing discovery requests and deposition questions.

The common consulting expert can also be of assistance when identifying testifying experts and preparing expert reports.

Furthermore, the testifying expert can access the universe of hosted ESI without compromising each individual defendant's attorney-client privilege and work product doctrine protections

Finally, hosting the expert's reports and supporting documents on the document management platform provides access to all counsel and secures the expert's work product.

Using Document Hosting Platforms for Collaboration

Document hosting platforms, in addition to facilitating the management and review of ESI, provide excellent tools for strategic collaboration among joint defendants.

First, they are useful when organizing ESI by subject matter, legal issues and testifying fact and expert witnesses.

Second, pleadings—which become voluminous during complex litigation—are maintained and easily retrievable by joint defendants and their counsel from a single location on which user access is common but partitioned among parties so that they may work independently as well as collaboratively.

Third, individual documents and pleadings can be downloaded easily by each joint defendant and annotated for particular purposes with the protection of the attorney work product doctrine; alternatively, modules may be built into numerous branded platforms for PDF markup collaboration.

Fourth, a common legal research repository can be created.

Fifth, the benefits of the hosting solution are enhanced when information is disseminated among the joint defendants through intra-platform, encrypted e-mail communication.

Lastly, a predictive coding module can be incorporated into the hosting platform for the benefit of all of the joint defendants.

Common Litigation Support; Establishing Audit Trails

''Audit trails'' concerning the collection and review of ESI may come into play if issues such as waiver of the attorney-client privilege, failure to produce documents, spoliation of evidence and obstruction of justice are raised.

Audit trails, demonstrated by an independent computer forensics expert may be critical, and therefore joint defendants can benefit legally and financially from the use of a common computer forensics expert who is certified by industry-recognized accredited forensic software providers to assist counsel.

Properly responding to SEC and DOJ proceedings is of paramount importance. A joint defense agreement will protect communications among counsel, and the bases for withholding ESI from production (i.e., the information and documents sought are not within the scope of the subpoena or are protected by a legal or statutory privilege).

  DDEE ISSN 1941-3882

The reasons for withholding ESI from production can be documented through use of current eDiscovery technology and services providers, and the documents withheld can easily be segregated and hosted.

In addition, the litigation support vendor can escrow a copy of the ESI withheld from production pending further action by the parties, including judicial intervention.

A computer forensics expert's testimony may ultimately assist all joint defendants when reasonable procedures for handling ESI must be demonstrated and key ESI is offered into evidence (e.g. establishment of a chain of custody for authentication).

Who Should Coordinate the Joint Defendants?

Dealing with different law firms participating in a joint defense agreement can be challenging. Personality traits and practice styles may cause friction.

Moreover, on a macro-economic level, many firms are placing a great deal of emphasis on the generation of legal fees.

Nevertheless, it is incumbent upon counsel to render advice which best advances the client's factual and legal defenses while reducing legal fees and costs, thereby affording maximum availability of insurance coverage.

In light of these objectives, appointment of counsel for one of the joint defendants as ''lead counsel'' is an important issue to consider when building the team. The manner in which this occurs must be transparent and collaborative so that each joint defendant is kept informed and allowed to participate fully.

Candidates for lead counsel in a multi-person joint defense of a complex legal proceeding should demonstrate the following skills:

- Knowledge and experience with respect to the types of legal proceedings, along with the state of the applicable rules of procedure and the government's applicable policies on exchange of ESI;
- Proficiency in managing review of large data sets;
- Familiarity with the landscape of litigation support vendors, eDiscovery consultants, and licensed forensics experts;
- Experience implementing early case assessment applications, and predictive coding modules where financially appropriate;
- Strong team-building and communication skills; and
- Negotiation skills necessary for resolving disputes which may arise among joint defendants and/or with other parties.

Lastly, but importantly, counsel appointed to ''lead'' the joint defense team as its ombudsman should be well respected by company counsel, the plaintiffs' bar, prosecutors and regulators.

Conclusion

Multi-defendant legal proceedings involving complex factual and legal issues litigated in civil, criminal and regulatory settings must be well coordinated and handled efficiently using state of art hosting platforms well supported by vendors and managed by counsel and computer forensics experts. Not doing so results in excessive legal fees and costs which waste insurance coverage.

A ''team leader'' is important for coordinating among the joint defendants so that the wheel is not continually being reinvented and counsel for the joint defendants are not operating exclusively within their own silos and taking different paths to the detriment of their clients and the group.