

Global & Domestic Compliance Readiness – Legal Service Providers

Managing e-Discovery And Avoiding Sanctions Under The FRCP Amendments

The Editor interviews **Brad Harris**, Director, Discovery Center of Excellence, Fios, Inc.

Editor: It has been one year since the amendment to the Federal Rules of Civil Procedure went into effect. What have you seen as the biggest impact or change in corporate legal departments as a result?

Harris: Since the amendments to the Federal Rules of Civil Procedure (FRCP) went into effect in December 2006 (and even before), the number one change we have seen is the an increased level of uncertainty and the fear of what might happen if changes are not made to how companies respond to e-discovery. At best, companies can continue to satisfactorily respond to discovery, but with higher costs and unpredictable outcomes as the response process is treated as a discrete event, often resulting in unnecessary fire drills. At worst, the company subjects itself to undue leverage and sanctions because it didn't do the right thing and can't defend its practices.

The more progressive legal departments are taking overt action to improve their electronic discovery readiness through assessment and planning. They are putting resources in place to gain better understanding of their electronically stored information (ESI) and data repositories. They are creating a dialogue with their IT department in which they discuss what business processes to put in place as a result of the changes. And they are creating formal discovery response plans to reduce the unpredictability of the discovery and mitigate risk.

One of the biggest changes as a result of the amendments has been the time frame for responding to a discovery request, which has become much more compressed and requires counsel to act much faster. Ninety-nine days from the time a suit is served in Federal Court is not enough time to do the proper planning on a large litigation matter or to develop a comprehensive e-discovery plan that can be used during negotiations with opposing counsel. This is further compounded by the fact that the scope of discovery has significantly expanded, along with the definition of what is subject to discovery – everything from e-mail to voice mail and proprietary files stored on databases.

Finally, the guidelines around what constitute good faith, under FRCP Rule 37, and how it is demonstrated is significantly different from what was expected by the courts just two years ago.

Editor: How has the meaning of and expectations around "good faith" changed?

Harris: Companies have always needed to show that they acted in good faith when responding to discovery or in response to any other court-ordered instruction; however, the burden of showing good faith is now significantly greater on the part of the responding party than it ever was before. Counsel can't claim that they didn't know about those back up tapes in a closet or that they didn't have proper access to IT personnel. Counsel needs to have proactive dialogues with ESI custodians and IT



Brad Harris

stewards. They need to create and maintain documentation regarding what preservation actions were taken when the obligation arose, how chain of custody was assured, and how both custodians and relevant ESI repositories were systematically identified.

Editor: What is the greatest risk with respect to compliance with the Federal Rules?

Harris: The greatest risk is, quite frankly, the failure to take action. There are a lot of companies that have gotten away with not having to do a lot of electronic discovery in the past or delay response at all in the hopes it would go away. The fact is that plaintiff attorneys have become savvier and are learning to use e-discovery to create leverage. Inaction can also expose a company to potential sanctions, which can be quite significant and costly, as well as increase the cost, risk and burden on the organization when response is required. This may result in confidential or privileged ESI being inadvertently produced (or not produced), critical evidence being destroyed, or too much evidence being collected and resulting in significant attorney review time and cost.

Editor: In terms of technology, there has been a lot of hype around review, e-mail archiving and technology solutions for e-discovery. What trends are you seeing? How can these technologies be leveraged for e-discovery success?

Harris: There are a lot of solutions being marketed in regard to e-discovery. From the standpoint of technology, there are software providers that are promulgating technology as the solution; however, it is important to recognize that technology is just one part of the solution. Before adopting or implementing a technology approach, counsel first needs to understand the people and processes necessary for responding to discovery. Technology may help make the response process more efficient and scalable, but only if it supports a consistent, repeatable discovery response process.

For example, several of our clients adopted e-mail archiving systems two or three years ago. These e-mail archiving systems, which are dedicated solutions

designed to automatically retain e-mail based on records retention policies across all employees, were considered state-of-the-art and the answer to both burgeoning retention and storage issues around ESI. Two years later, these same companies are now evaluating and purchasing new systems because the original ones have proven to be too burdensome and limited in their ability to extract ESI when required for discovery response.

Companies need to focus first on the process in deciding what needs to be retained, why it is being retained, and the requirements around accessing the data once in storage. Based on those requirements, and the overall business needs of the organization, then technology can be leveraged to make e-discovery response more cost-effective and efficient.

Editor: In order to be "e-discovery compliant," what two or three actions do you recommend corporate counsel take as highest priority?

Harris: First, focus on process that assures transparency and good faith. What are the company's current processes for responding to discovery requests? Where do the greatest gaps lie between current practices and industry "best practices"? What improvements can be made, both short- and long-term, to ensure compliance with the Federal Rules? Once the gaps have been identified, develop a formal plan that includes actions to close those gaps. Not only will this help galvanize the e-discovery response team, so that there are consistent practices that are predictable and measurable, it will also help the company more easily demonstrate good faith behavior by documenting improvements in process.

Second, understand the company's IT infrastructure. From the time of *Zubulake* to the current *Qualcomm v. Broadcom* battle, it has become apparent that counsel needs to be familiar with the computer systems and the IT infrastructure of the company. Take action now to understand what applications and content repositories exist throughout the company. Work with IT to identify how ESI is retained and stored. Learn what type of files and information is stored in each repository and how the content is governed. Such an ESI content mapping process can start with a specific matter, or be based on a company's overall litigation portfolio. Either way, this will help counsel understand how ESI is being captured, retained, and ultimately disposed in the normal course of business, as well as weigh what will happen if no action to preserve is taken.

Third, develop an ongoing dialogue between IT, records management and legal, starting with language and expectations. This will help establish a common understanding of technology and legal risk, especially when called to identify, preserve and collect ESI for discovery.

Editor: In bridging the communication gap between legal and IT, what infrastructure or process changes should general counsel be considering?

Harris: We see the value of putting in place dedicated resources, such as Tech-

nology Counsel or e-Discovery Counsel, who have expertise in both legal discovery and IT. The more progressive legal departments are already doing so – either by establishing a multi-disciplinary team or by assigning a dedicated resource that understands both the legal and technical requirements around e-discovery.

From a strategic perspective, a Technology Counsel will be able to lead the discussions around what types of processes are in place for responding to discovery and the impact of technology on the process. From a tactical perspective, when there is a need to respond to a preservation obligation or e-discovery request, the Technology Counsel can ensure the processes around identifying relevant custodians and issuing legal holds are done consistently and in compliance with corporate and legal policies.

Finally, the Technology Counsel can serve as the resident expert and direct appropriate behavior when discovery obligations arise. Establishing this role will help bridge the gap between legal and IT, as well as ensure the company is in compliance with the FRCP, court-ordered mandates and other governmental regulations.

Editor: Fios offers comprehensive consulting services around information governance and electronic discovery compliance. What other steps should corporate counsel take to help improve practices relating to information governance and e-discovery response?

Harris: Compliance with the FRCP, ensuring policies are effectively enforced cross-departmentally, leveraging technology to improve processes, and improving communication between legal and IT all comes down to the defensible and predictable management of ESI. This Information Governance means taking actions specifically devoted to improving the way ESI is captured, retained and managed.

Fios has experience in developing programs to reduce the cost, risk and time associated with all phases of the process. As part of this planning, we help clients identify methodologies for retaining information that has business value and eliminating the information that does not. Our goal is also to improve the way information is organized and structured, so that both IT and legal can understand what content exists, how it is structured, and how accessibility can be improved. This is particularly important in the early stages of discovery – identification, preservation and collection – as this is where most companies make the biggest mistakes (i.e. Morgan Stanley, Intel, & Zubulake).

Companies need to start with a six- to 12-month review of records management policies and analyze how current policies get implemented and what practices are in place to insure compliance when legal holds are required or when they expire. For example, with the e-mail archiving, does the system have the ability to place a hold by custodian or only by server? It all gets back to focusing on processes and procedures and doing it in the context of e-discovery risk. Focus on processes that produce the highest returns and the greatest chance of success for both the company and its shareholders.

Please email the interviewee at bharris@fiosinc.com with questions about this interview.