AVOIDING "FAUX" E-DISCOVERY

How A System-Based Approach Reduces Your Risk

By James D. Shook, Esq.
Andrew M. Cohen, Esq.

Companies reviewing their electronic discovery options are frequently faced with a difficult choice on how to implement litigation holds and collect relevant electronic information. At first glance, the choice seems to be a "Catch-22": should they: (a) quickly and inexpensively implement an employee self-service approach, and accept the inherent risks of such an approach; or (b) spend time and effort up-front to deploy tools that will systematically allow an investigator or legal team member to identify and collect the information?

There is no easy answer – in part because every company has different litigation volumes, tolerance for risk and budgets for litigation, electronic discovery and IT. Moreover, both approaches, if implemented correctly, are

Human nature can undermine the entire self-service process.

likely to be acceptable to most courts. However, there is a significant amount of risk and difficulty hidden in the self-service approach, which can lead to "faux eDiscovery"– where a company incorrectly believes that it is meeting its electronic discovery obligations. This article will identify and explore some of those risks, assess the system-oriented approach and offer a roadmap for improvement.

The "Honor System" and Its Risks

Companies implementing a self-service approach for electronic discovery basically rely on the "honor system" in asking their employees to preserve and collect information that may be relevant to a matter. While this approach can be effective in some cases, it is fraught with risk and problems.

The self-service process typically begins with a notice from the legal department to all employees who are either a focus of the case or have been identified as likely to have discoverable information. Sometimes the notice will simply inform these "custodians" that they may have information relevant to a matter, and that this information must not be deleted. As an additional safety measure, some notices may direct the employee custodians to not delete <u>any</u> information. Or the notice may even require the employee to review all electronic information – email messages, files stored on the desktop, laptop or fileshares where the employee has access, etc. – and to move or "copy" any potentially relevant information to a separate folder specially created for the litigation matter. (The folder may be created by the employee on the desktop or may be a link to a secure fileshare located on a network storage system).

While on the surface this process appears simple and easy to implement, it is deceptively difficult. Many potential issues and problems lurk just beneath the surface and are generally based on two factors: human nature and technology.

> **Even for employees that are able to set aside self-interest, a skilled adversary may use the possible self-interest to call the entire process into question.**

Human nature can undermine the entire self-service process. A key issue in this area involves the employee's potential level of self-interest in the case. For example, will an employee attempt to delete relevant information that might be embarrassing or that tends to paint the employee in an unkind light? Even for employees that are able to set aside self-interest, a skilled adversary may use the possible self-interest to call the entire process into question. The opposite problem is also an issue – an employee may be completely uninterested in the case and ignore the notice from legal, or complete the work in a haphazard manner.

There are also many technology-specific risks involved in a self-service process. Most employees will not have an extensive knowledge of their IT infrastructures, and may not even understand how to preserve all of their electronic information if they can find where it is located. For example, in the electronic discovery dispute in the litigation between AMD and Intel, not surprisingly, some employees were not fully informed about the need to preserve emails within a certain timeframe before they were automatically deleted.[1] Even when electronic information is properly saved, files are typically collected through a "drag-and-drop" process to a folder, which may change some of the important system metadata such as the dates the files were modified, accessed and created.

In many cases, concerns about these issues result in the process being handed over to the IT team, which is able to apply its more extensive knowledge of systems and the company's infrastructure to the process. This may cure some issues but usually results in the creation of entirely new problems, such as an overly inclusive process, where entire laptops/desktops and even fileshares are imaged. In turn, this creates a significant over-preservation of data, substantially increasing the overall costs of electronic discovery. The process can also result in "faux eDiscovery" – where the IT department, not understanding all of the legal issues, simply does not collect all discoverable ESI, with the legal department blissfully unaware – until an adversary points out their flaw.

A Better Approach

A system-focused approach substantially reduces or eliminates reliance on individual employees holding and collecting their own data. With this approach, a company deploys infrastructure and tools enabling an investigator to search through its systems, place relevant, discoverable data on hold, and ultimately collect and store the data for further processing.

These system-oriented tools can take many different shapes and sizes. For example, email archiving systems can help to aggregate email in a central collection point, including the elimination of distributed (and unman-

aged) local stores of email like the ubiquitous Microsoft Exchange Personal Storage Table or "PST" file. Increasingly, companies are also leveraging low impact "collection appliances" that feature the ability to be almost immediately deployed. These tools index file and email content so that more efficient collections and policy management strategies can be employed. Once content has been identified as relevant to a particular matter, it can be easily copied to a repository, in a legally sound manner, and sequestered for preservation or further processing and production.

The system-oriented process addresses the risks inherent in the employee-focused system. People familiar with the technology and the legal requirements perform the litigation hold and collection process instead of potentially self-interested (or completely disinterested) employees. With appropriate training of this team, typically stocked with both IT and legal experience or at minimum key input from the company's legal and IT teams, potentially relevant data throughout the enterprise is more likely to be considered and protected. Finally, with appropriate tools and training, the data is collected in a manner that maintains and protects metadata and chain of custody where appropriate.

All of these benefits create significant value for the company. Complete and responsible collections substantially reduce the risk of incomplete work that can lead to expensive and risky claims of spoliation. In addition, such tools may enable the litigation team to evaluate the case at an early stage, resulting in an early risk assessment that can reduce overall costs through settling "bad" cases earlier in the process. Perhaps most importantly, these tools enable more efficient search and deduplication, leading to smaller result sets and the potential for significant costs savings because less content is being processed and reviewed downstream.

Phasing In

Many companies initially deploy an employee-based self-service model, and then, recognizing the enhanced risk of litigation or merely becoming more educated in the risks of the system, take a phased approach toward implementing system-focused tools. Done correctly, this approach blends the effectiveness of a strong hold notification process, which is usually part of the self-service model and a key component of any good electronic discovery strategy, with more systematic approaches to preservation and collection.

> **A system-focused approach substantially reduces or eliminates reliance on individual employees holding and collecting their own data.**

A common first step towards a system approach is to deploy Email Archiving infrastructure, with centralized (and enforced) email retention policies, to enable systemized review and collection of email. Follow-on steps may include "collection appliances", document and records management systems, evaluation of a company's information repositories, litigation hold workflow and even review tools – but all must be based upon a holistic assessment of the company's infrastructure and needs. It is extremely important to have a complete picture – even if not fully detailed – before embarking on this phased approach.

To reduce risk during this transition period, companies

may consider adding some of the following steps to their traditional employee-focused approach:

- More detailed notifications to employees about the subject case, examples of systems to consider in making their self-evaluation, and where to go for additional information or assistance;

- A one-to-one follow-up from a legal department representative, at least for "key" custodians;

- In-person or telephone and computer-based oversight (WebEx, NetMeeting, etc.) from a legal representative during the identification and collection process;

- Additional training, potentially computer-based, to educate employees on their litigation hold responsibilities and on how to best discharge this obligation;

- Requiring affidavits from employees during the litigation hold and collection process, certifying that the employee has fully complied with its obligations. While the usefulness of such affidavits may be questionable in court, it should insure that employees give the process their full attention;

- Create a sufficiently broad circle of interest for the initial notification process. Since information is not being systematically saved from custodians who have not been notified, this will help to avoid spoliation claims;

- Consider providing similar notifications to owners of company systems, such as archive, backup, content management, email, etc., so that data not under an employee's direct control can be preserved as necessary.

> **The employee-focused, self-service discovery process has been a mainstay of the litigation process.**

Conclusion

The employee-focused, self-service discovery process has been a mainstay of the litigation process. While not perfect, the process worked well in the paper-based world and has also been acceptable for the early stages of electronic discovery. However, the complexity of today's IT systems and the stringent requirements for electronic discovery render it mostly outdated. To date, most electronic discovery has focused upon email but is rapidly moving to unstructured data and even larger systems. Companies that continue to rely exclusively upon an employee-oriented approach for electronic discovery face risks that will continue to mount, and should consider a more system-oriented approach.

---

[1] In Re Intel Corp. Microprocessor Antitrust Litigation, MDL Docket No. 05-1717-JJF, Civil Action No. 05-441-JJF, US District Court (Delaware).

EMC²
where information lives®