Today's
GENERAL COUNSEL
JUNE/JULY 2013 VOLUME 10/NUMBER 3 TODAYSGENERALCOUNSEL.COM

Practical Tips For Managing E-Discovery

By Jasmine Juteau

As companies attempt to rein in legal fees, many are considering tackling more e-discovery tasks in-house, and corporate counsel are finding they need to have greater insight into the e-discovery process. This article is a practical guide to various e-discovery issues facing companies today, written with corporate counsel in mind. It addresses current topics in the preservation, collection and review of electronically stored information (ESI). Careful thought and advance planning in these areas can help counsel achieve maximum compliance with minimum risk, cost and interference in business operations.

THE LITIGATION HOLD

After receiving a demand for ESI, the first step is to initiate a procedure for preserving relevant materials. To prepare appropriate litigation hold instructions for custodians and IT employees, there are several questions to ask:

- Who are the custodians?
- What are the dates for requested information?
- What is the relevant ESI (e.g., email, databases, or other

electronic files)?
- Where is ESI stored?
- How is it backed up or archived?
- Does the company have data retention policies or other practices, and if so should they be altered to accommodate preservation?

Detailed responses to these questions will form the backbone of instructions provided with respect to ESI retention.

Don't assume the company server houses all relevant ESI. For example, counsel often overlook local storage. Files saved to a computer desktop may not be saved to the network, in which case "images" of the hard drives may be required.

The number of devices used by employees has multiplied, so it has become necessary to be aware of ESI stored on devices outside the office. Ask whether custodians work remotely and have laptops, home computers or personal data archives with relevant information. Ask if they use smart phones or other personal devices (like tablets or e-readers) for work purposes. Consider whether they use third-party providers which host ESI (e.g. on-line email accounts, instant messaging or file sharing services).

Even information that is outside the office may be within the company's "custody or control." Several courts have determined that companies have a legal right to company information saved on an employee's personal computer or in a personal account, and the company can require the employee to furnish that information in response to a document demand.

Similarly, several decisions have established that where the terms and conditions of a third-party service establishes the company's authority over the relevant data, the company is responsible for requesting and producing such data in response to a document demand.

BACK-UPS AND RETENTION

Back-up and archiving practices are changing rapidly. As the volume of data expands, back-up tapes are being replaced with back-up servers and cloud-based storage, including vault systems. These systems offer far greater capacity and provide easier access to stored information if needed – and they present yet another source of ESI.

Most of this data will duplicate the ESI on the "live" network, but it is important to understand the precise relationship between them. For example, archive systems may capture only certain portions of documents, so the live network version is more complete. To issue an effective litigation hold and ensure a complete collection, IT professionals should be consulted about the relevant differences, if any, between the archived information and the live network.

IT professionals and the custodians should also be consulted about policies or practices employed to limit data storage. Any "auto-delete" function, whether system-wide or applied on an individual basis, should be immediately disabled for relevant custodians. Similarly, the company should know the deletion practices of its third-party providers and take immediate steps to gather information in danger of being purged. For instance, some services maintain client messages for five years. If a subpoena was served today regarding activities that took place in 2008, potentially relevant communications would disappear daily without intervention.

A further consideration for companies with international offices is the geographic location of ESI. Global data networks allow employees in one country to run email or access files on servers in another country. Meanwhile, countries are promulgating data privacy laws that limit the ability of local offices to transfer personal data such as employee email abroad, even to corporate affiliates or company attorneys.

In a recent example, the Macau Office for Personal Data Protection penalized the Macau unit of the Las Vegas Sands Corp. for the unauthorized transfer of customer data to the U.S. parent company. If relevant ESI resides abroad, companies must carefully consider the potential impact of data privacy laws.

Once ESI has been identified and secured, the next step is organizing the collection of data for review and, ultimately, production. There are several compelling reasons for ensuring that all relevant ESI is collected and reviewed in a sound and orderly fashion. An insufficient collection effort can quickly escalate into a series of problems. Counsel's ability to conduct an early case assessment and consider the company's position may be hampered without timely identification of key documents.

Failure to conduct a complete collection also will mean more collection work in the future, with more delay and disruption to the company. In addition, metadata, the background electronic file data that is generally required in response to the document demand and could be important evidence, may be corrupted or lost without a forensically sound collection. By saving and exporting data without the proper software or training, in-house IT professionals can permanently alter this critical information.

Lastly, insufficient or incomplete collection can lead to costly discovery disputes and, in the worst cases, sanctions for spoliation.

VAULT SYSTEMS

Many companies use so-called "vault" systems for data storage and archiving, and these systems are also marketed for e-discovery, particularly to facilitate in-house collection and review. There are several benefits to vault systems, such as the capacity to maintain a complete set of all network data, the capacity to safeguard metadata, and advanced search functions. However, it is important to understand their limitations for e-discovery purposes.

There are several technical issues for counsel to consider before authorizing ESI collection using any in-house resources, including a vault system:

- Will the in-house personnel design

and input search instructions appropriate to the system and sufficient to capture the desired results?
- Will the searches include documents in their most complete form, such as emails plus their attachments, or databases plus underlying data sources?
- How will the company address ESI that is not stored on the network or vault system?
- When extracting data, what impact if any will there be on the files' metadata?

Counsel should also consider whether a vault system offers a viable alternative as a document review platform. Features such as de-duplication of identical emails, the ability to review related emails as a group, capacity for multiple reviewers and retention of document review history are all relevant to that assessment. It is essential to have a complete understanding of the benefits and limits of vault systems before utilizing one for purposes of e-discovery.

While new technologies such as predictive coding are gaining ground, they remain cost-prohibitive for most standard e-discovery needs. The traditional method of designing and applying search terms continues to be the preferred method of reducing a large collection of ESI to a manageable review set. Designing a search that will achieve a well-tailored set of potentially responsive ESI is a crucial task. The terms must be broad enough to capture all potentially relevant materials without pulling in an abundance of false positives and irrelevant documents.

As ESI multiplies, crafting precise and accurate terms is an important aspect of cost-saving. Moreover, judges routinely criticize discovery efforts based on poorly-selected search terms, and they have recommended that attorneys consult with professionals qualified to design an effective search methodology.

Identifying and drafting relevant search parameters involves several steps.

- Understand the search function of the relevant software.
- Speak with key custodians to assess the subject matter and identify key terms, including common abbreviations and shorthand references.
- Review key documents to identify core terms and concepts.
- Control quality to judge initial search results and adjust search terms as needed.
- When possible, cooperate with opposing counsel on the search to avoid later disputes.

Failure to follow these steps can result not only in an overly costly and burdensome review project. It can also lead to deficient production that is subject to sanctions. ■

Jasmine Juteau is Counsel to Morvillo Abramowitz Grand Iason & Anello P.C. Her practice is focused on white collar defense, regulatory enforcement and corporate compliance.
jjuteau@maglaw.com