LJN LAW JOURNAL NEWSLETTERS

LJN'S LEGAL TECH Newsletter®

An ALM Publication

Volume 27, Number 9 • January 2011

How Legal IT Can Avoid the Pitfalls of Risky ESI Collections

By Alon Israely, Esq., CISSP

In almost every respect, e-discovery falls squarely in the domain of attorneys — inside counsel, outside counsel and experts. Essentially, it is the business process for litigation, regulatory matters and internal investigations. So why is IT involved in almost every situation? The answer is quite simple: because IT *must* be involved. Today, the information used and relied upon by attorneys is digital. Documents created by users (custodians) that are a part of litigation or regulatory matters live and die in electronic form and are stored on information systems — managed, serviced and controlled in large part by IT.

But with law firms and corporations tightening budget belts, IT organizations that are supporting legal teams to preserve and gather (collect) data are tempted to perform those tasks in ways that do not meet the standards required by the current legal rules.

No Quick Fix

Under the time pressures brought on by litigation and regulatory investigations, utilizing quick-and-dirty methods — such as self- and ad-hoc collections, bulk copies and exports — may at the outset seem to be cheaper and more convenient, but ultimately carry serious legal risks. IT is responsible to ensure that the organization does not face legal sanctions because of the way in which data was gathered and transferred.

Thus, the mechanics of identifying, gathering and transferring information for eventual use as possible evidence requires technical savvy and local IT knowledge, but importantly also requires knowledge regarding the principles to follow — many based in computer forensics and information security — to ensure that the manner in which the data is handled is compliant with the related legal requirements throughout the data gathering process.

Individuals in IT who support the legal department and outside attorneys are a critical part of the "data team" that comprises the technology side of the discovery process, primarily related to preserving, gathering and managing the electronically stored information (ESI) possibly relevant to the legal matter at hand. They have the not-so-easy job of coordinating the mechanics of the process to gather e-mails, documents and structured data from the rest of the organization — employees (*i.e.*, users), departments, vendors, affiliates and others who touch the IT systems such that they may be implicated as custodians in any number of legal matters with which the organization is involved.

But in many cases, the IT organization, tasked with assisting the attorneys, is not prepared to reliably and confidently handle ESI collection activities in a defensible, accurate and cost-effective way.

Primarily, IT operational goals are at odds with those of good e-discovery collections. Well-managed IT requires efficiencies and automation that tend to get in the way of complying with many legal requirements related to data preservation and collection. For example, a typical procedure used to export data from a system or a standard bulk file copy process may truncate or alter the data in a way that it has no bearing on normal business activity, but causes failure in compliance with discovery rules.

To make matters worse, IT systems never exist in a utopian state or in a vacuum; they are dynamic and contain a multitude of technical challenges for maintaining relatively good normal operations. Those challenges multiply greatly when IT activities are performed to facilitate e-discovery.

Thus, because of a lack of training, planning and appropriate tools and methods, it is often easier for IT staff involved in ESI preservation and collection activities to rely on IT style "efficiencies" to get data from point "A" (users/custodians) to point "B" (the attorneys). But that is a dangerous course as IT is called upon to answer questions regarding data integrity, consistency of process and potential spoliation claims.

IT and Legal Challenges

Some typical perilous scenarios for IT include situations where IT sends normal copies of data across volumes to be transferred via external storage to a vendor for processing (for example, in organizations with e-mail archiving systems), where e-mail is gathered by setting up forwarding rules or without regard for stubbing issues, open source conversion tools are used against exported record sets, and users are instructed to move or copy relevant files to a shared folder from where the documents are normally stored. According to Federal Rule of Civil Procedure (FRCP) 34(b)(2)(E), a party must produce documents as they are kept in the usual course of business or must organize and label them to correspond to the categories in the request. Whenever documents are altered beyond the format in which they are

Alon Israely, Esq., CISSP, is a senior adviser at BIA, an electronic discovery products and services company headquartered in New York City. He may be reached at aisraely@biapro tect.com.

stored in ordinary daily operations, there is a maximum point of concern as to the data's integrity.

As IT personnel gather the bits that lawyers need to use, they are stymied by the requirement to use the correct methods, tools and processes to ensure compliance with data preservation and handling legal requirements. Typical IT data transfer activities do not meet the higher standards that the law requires.

But to be clear, this is not solely a problem of using the wrong technology, but it is about using the required techniques and related processes that include following a well-vetted plan involving users, maintaining logs and auditability, and certification of workflow by the attorneys. Those additional requirements create the need to be aware of certain details that are not normally considered in performing typical IT business operations.

Using the correct supplemental processes to ensure data integrity and compliance with legal obligations requires special procedures be followed, including a known plan, training, upkeep of those procedures and quality control processes — all of which add more overhead to the entire IT process.

It takes expertise and experience to design those procedures, and time and training to implement and maintain them, but they are critical to successful e-discovery compliance. Law firms and their corporate clients that invest the time and resources to establish those types of procedures ultimately spend less money and time on preservation and collection activities, while still maintaining a defensible stance in their e-discovery activities.

Defensible ESI Collections

To collect ESI for legal purposes in a manner that complies with the current standards of discovery, several fundamental principles must be in place and followed. These fundamental principles include ensuring data integrity, maintaining auditability and following well-vetted standard operating procedures.

Proper e-discovery procedures dictate the participation of users (custodians) for some parts of the data identification process, following a protocol to identify relevant systems, data types and time frames, working under the ultimate supervision of the attorneys and maintaining auditability.

Though involving users creates challenges to automating the overall ESI collection process and hampers efficiency, doing so is important in light of recent case law that considers whether interviews have occurred, and because, in most cases, the users themselves have the most knowledge with respect to where they keep relevant documents. In many cases, a simple questionnaire used to gather responses regarding where data is stored is the best way to proceed but requires reconciliation and quality control. A good process will help maintain efficiencies around that and will lead to more targeted collections that create savings down the road.

It is critically important to follow a protocol when identifying and gathering data from users, as that creates consistency and accuracy around the process. A collection protocol defines what to collect, such as which file types (*e.g.*, business productivity files such as MS Word documents, Adobe PDF documents and MS Excel files), the relevant date ranges (if any) and which date fields on which to rely and from where to collect (*e.g.*, what storage areas and from which systems). Protocols must be written and can be used by IT to drive automation in the mechanics of the data gathering process.

Attorney supervision is required, since the gathered data and procedures used must ultimately be defensible. The attorneys representing the issues and facts in the legal matter may rely with confidence on the integrity of the data and diligence of the process. Also, the development of the protocols stated above and the enforcement plan of the overall procedures used in the e-discovery process must involve in-house counsel or outside legal consultants.

Thus, using the correct appropriate specialized tools to identify, copy and transfer data for legal matters and the procedures used to manage and guide those IT processes lead to successful ESI preservations and collections, obviating the need to resort to risky non-compliant, ad-hoc processes while still maintaining efficiencies and cost-controls.

If IT does not gather identify and collect the data correctly, then the rest of the legal/discovery/investigatory process may suffer.

By using typical IT shortcuts and standard IT tools without regard for auditability or data validation, and by not following the correct e-discovery collection procedures, risks abound. Those include the risk of altering or destroying file system metadata, and the risk of truncating critical information. By ignoring accepted industry standards and employing inefficient collection methods, IT may incur unnecessary costs, or become vulnerable to witness testimony and the inherent risks of inconsistent data preservation and collection methods.

Conclusion

Legal IT departments are subject to a great deal of training in their own tools, techniques and procedures. However, this knowledge does not necessarily apply the same way when it comes to completing a defensible collection of ESI for e-discovery purposes. However, by educating themselves about ESI collection techniques and by working closely with the outside and/or inside counsel to get the attorneys' perspective on the importance of the possible evidence, then legal IT can be more nimble and avoid the pitfalls of self-collection in order to produce data that is pristine and useful at the same time.

BIA
39 Broadway, 26th Floor
New York, NY 10006

Toll Free: 1-888-338-4242
Email: pr@biaprotect.com