Woman Advocate
FROM THE SECTION OF LITIGATION WOMAN ADVOCATE COMMITTEE

The Risks of Electronic Data Over-Preservation

By Anne Kershaw and Shannon Spangler – May 25, 2012

Picture this: You're the risk-management partner for an AmLaw 200 law firm. Sheila, leader of your litigation team, comes to you for advice. A year ago, she won a defense verdict in federal court for a corporate client. After the verdict, the case settled quickly for waiver of costs. Because the company and Sheila reasonably believed this was a one-off case, your firm advised the client that it could dissolve the legal hold and manage its documents and data pursuant to its usual retention policies. The client appropriately disposed of many of the electronic documents that were produced in the first case.

Three months ago, a different plaintiff filed a nearly identical lawsuit, proving Sheila and her client wrong about the likelihood of repetition. The client issued a new, but nearly identical, legal-hold notice for the second lawsuit. Predictably, the plaintiff served the same document requests that were served in the first case. You know that the advice regarding dissolving the legal hold and returning to normal document retention policies was sound and well documented, and the legal hold for the second case was timely issued.

It turns out, though, that your firm *still* has multiple copies of the very documents that the client disposed of post-litigation. After the first lawsuit ended, your litigation colleagues moved on, not giving a thought to the firm's file-closeout procedures. Must Sheila tell the client about these copies? And must the client produce them in this new lawsuit? After all, as far as the client is concerned, they no longer exist, and there wasn't any obligation to retain them between the first and second lawsuits.

You remind Sheila that even though the company (and thus your firm) had no obligation to retain these documents after the first lawsuit ended, the current legal-hold obligation trumps the right to dispose. In short, if the documents now exist, they likely must be disclosed if they are potentially relevant under Fed. R. Civ. P. 26(a), 26(b)(1) and 26(b)(2)(B), and possibly produced under Fed. R. Civ. P. 34. In addition, lawyers who know of documents preserved for one case that are relevant in another have a duty under Rule 26(g) to disclose the existence of those records.

Of course, now that the client knows about these documents, it claims that your firm is responsible for all costs and liabilities relating to the improper retention of these documents. Is this claim covered under your firm's professional liability policy? You may face a coverage dispute in addition to the suit filed by your former client. You may

also have violated attorney ethics rules. All this because no one took the time to properly and completely close the matter and manage the documents.

Many recent articles address businesses' habit of data hoarding—routinely storing vast amounts of electronic data (and perhaps paper) they are neither required to keep by law nor have a business need to save. *See*, *e.g.*, Anne Kershaw, "What Lurks Within," *Law Technology News*, December 1, 2011 [visited April 22, 2012]; John Chapras II, "Auld Lange Syne New Year's Resolution," *Law Technology News*, December 1, 2011 [visited April 22, 2012]; *Survey Finds Infinite Data Retention Leading to Costly Information Management Mistakes*, Symantec, August 4, 2010 [visited April 22, 2012]; Matthew Minor, "Alignment of Document Retention and Litigation Hold Strategies Is Key to Defensible Data Deletion," *EzineArticles*, February 13, 2012 [visited April 22, 2012]. Business executives and their lawyers worry that the data contains information that *might* be subject to a legal hold or relevant to some existing or as yet unknown future litigation, and its disposition *might* be second-guessed by adversaries and courts. Many are reluctant to throw it out and risk spoliation sanctions, even if that risk is remote, but saving everything to avoid sanctions is not an insurance policy; to the contrary, it increases risk.

In corporations, we find that 80 percent of ostensibly "active" files and folders on hard drives and in file shares have not been accessed for 3–5 years. In other words, 80 percent of the electronic files are essentially dead—yet IT spends money on these dead data daily for infrastructure, disaster recovery, and data migration as old servers and systems are retired. Some organizations also pay to store tens of thousands of backup tapes, all essentially useless. Other costs are hidden, such as lost attorney and paralegal time spent wading through unused and unwanted information to find what they need.

Law firms are not immune from similar over-saving of data with little to no future value. While law firms will recognize the business case for properly managing their own data to avoid the obvious operational costs associated with data maintenance and storage, the most visible costs associated with data hoarding can be legal expenses. Document review is often the largest single expense in litigation, and it can quickly mount to hundreds of thousands of dollars, if not millions. When it comes to a law firm's administrative data—such as law firm financial records and employee files—the risks of over saving likely are indistinguishable from those that any business might embrace by keeping unneeded data.

Special problems arise for law firms holding client information and documents transmitted to or created by the law firm in connection with the representation. These could be company business documents provided for purposes of conducting an investigation, for fact development in litigation, or for review and production in discovery. The documents and data provided to the law firm are likely to be copies, but it is possible for law firms to either hold or create unique client documents—for example, through addition of notations. Law firm case files also may contain documents generated for the client that "belong" to the client under applicable state law. *See*, *e.g.*,Julie J. Colgan, *The Ethical Custodian – aka The Messy Truth About Records & Information Management in Law Firms*, eLegalTechnology.org, [visited April 22, 2012]. No attorney

would intentionally create significant e-discovery issues for a client and possibly liability issues for the firm, but law firms may end up in the same place through inattention—by failing to implement and follow case-file closing and records-management procedures. In short, law firms should dispose of data when it is eligible for disposition, before a matter arises, thus minimizing the risk of incurring these potential costs and liabilities.

What is your firm's data-hoarding quotient? Do you know what client data you have and where it is stored? Do you faithfully attend to post-litigation or post-engagement file-close-out procedures and counsel your clients regarding appropriate disposition of electronic data? Are you experienced in counseling on both the technological and legal aspects of electronic data and e-discovery, and do you have professional-liability coverage for data-disposal recommendations?

Your firm could decide to meet its obligations—and the clients' expectations—regarding law-firm-maintained data by counseling your partners regarding the risks associated with retaining data they should not keep and the possible professional-liability-coverage gap for document-disposition recommendations. A better approach, however, is for the law firm to launch a workable and cost-effective electronic-data housecleaning program to evaluate its data-retention practices and dispose of both administrative and client data that are not legally required to be held and serve no ongoing business purpose.

A first step is to review the firm's records policies and evaluate how they apply to both its own administrative data and any client records it may have in its files. Do the policies specifically cover electronic information? Do they address client data and prescribe post-litigation and/or post-representation document-management procedures, including protocols to properly dispose of data in the hands of the law firm and other third-party vendors? Is the management of client data addressed in engagement letters, and are those provisions regularly followed?

Next, map the firm's data systems and inventory the data it holds. Active firm data is likely held in numerous places, including file shares and email folders. In addition, the firm should identify its legacy data sources, such as hard drives, servers, archives, and/or back-up disaster-recovery tapes. And, don't forget about third-party vendors and opposing counsel. Into what other hands has the firm or the client put client data? This step is often best completed by simply issuing a survey within the firm.

Once the firm has a good grip on what it has and where, it should identify, by folder or container, data that is transitory and eligible for deletion versus data that is subject to a records-retention schedule or otherwise must be held for legal reasons or in connection with an active client matter. Different processes may apply for different types of data but the review should not, for the most part, be done document by document. For example, folders in file shares should be reviewed to determine the dates of last use of the folders and files. The search functions now available in operating and email systems can be used to search categories of records that need to be retained. Physical data containers like drives, servers, tapes, and other media should be inventoried and reasonable efforts

should be made to determine their provenance and whether they are duplicates of data held elsewhere.

In short, if the firm continues to hold client data beyond the expiration of a particular legal-hold obligation, the law firm should immediately contact the client to discuss appropriate disposition. Your clients will love you for doing this. Factors that may impact the ultimate decision include the likelihood of like-kind litigation in the future; whether other copies of the data exist; whether it is inaccessible; and whether it is commingled with other client or firm data. The firm should employ the same processes for its own administrative data, retaining that which is required for business, regulatory, or legal-hold purposes and disposing of the rest. As to both client and firm data, it is critical to fully document both the evaluative processes you followed and the decisions you made. This documentation may include data maps; employee surveys; inventory lists; memoranda documenting conversations with key IT personnel, firm lawyers, paralegals, and client representatives regarding the content of various repositories; and notations regarding ultimate dispositions.

Finally, the firm must give serious consideration to whether it has the capacity, expertise, and risk tolerance to do the housecleaning effort described above or whether it should seek outside assistance. First, is the firm willing to make the internal investment required to do a meaningful housecleaning? It may not be possible, or economical, to dedicate resources to a project of this magnitude.

Second, does the law firm have the requisite expertise? Judges and academics speak more and more often about the question of e-discovery competency. *See*, *e.g.*, YouTube interview with Judge Facciola and Michael Arkfeld, [visited April 22, 2012]. The ABA Commission on Ethics 20/20 issued "Revised Draft Resolutions for Comment — Technology and Confidentiality," [PDF] in February 2012. Among other things, this draft adds to the Comments following Rule 1.1, under the heading Maintaining Competence: **"**[6] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with technology . . . ."

Expertise and risk are likely inversely related. But there are other factors to weigh. Will the law firm's professional-liability insurance cover decisions it makes about data and document disposals? In addition, as noted above, documentation of the law firm's housecleaning is critical to a defensible process. How the firm staffs the work may have an impact on whether or not internal documents created during the project are subject to privilege protections.

An experienced and properly insured outside consultant or expert, willing to provide an opinion letter verifying the reasonableness of the firm's processes and recommending the final disposition of records, can bring significant value to the process. A number of factors will shape the scope of the consultant's engagement, including whether it is appropriate for the consultant to have access to a client's confidential materials. In

situations where it is not, the consultant's role may be limited with respect to determining the provenance of data and making specific disposal recommendations. Even then, though, the consultant can bring significant value in terms of planning, documentation, and verification. Having a legacy data-management expert lead the effort will help ensure that the processes and results are properly documented and that applicable privileges are protected should disposition decisions be questioned later. In this scenario, it is the consultant and not litigation counsel who would likely be subject to deposition. Shifting the burden in this way can be both effective and comforting for the law firm and its clients.

Keywords: litigation, woman advocate, document preservation, litigation hold, professional liability

Anne Kershaw is a principal of A. Kershaw, PC/Attorneys and Consultants and cofounder of the e-discovery Institute in Tarrytown, N.Y. Shannon Spangler is an attorney and consultant who most recently served as vice president and associate general counsel for a Fortune 500 company.