

TechnoFeature™

Practice management and technology articles written by experts.

eDiscovery: Everything You Need to Know About Records Management, Identification, and Preservation — Part 1 of 2

By Bruce A. Olson

INTRODUCTION

In this new era of eDiscovery, the role of an attorney is much different than previous times. You no longer have the luxury of waiting until a client has decided to sue or has been sued to determine what electronic information about a particular disputed matter exists, or where such information is located.

The obligation to preserve electronically stored information (ESI) arises when you or your client have a reasonable expectation that litigation will ensue. What that "reasonable expectation" is varies from case to case. In some businesses that expectation is always present. If you represent a potential plaintiff the obligation to preserve may well arise before you are even sure you have a case, or your client has decided he/she actually wants you to commence litigation. You can't start sending out demand letters or conducting settlement negotiations just to see how far you can get short of filing a lawsuit, without taking appropriate steps to preserve your client's ESI.

On the flip side, if you receive a demand letter you can't just wait and see what happens, or do nothing until your client is actually sued, before you initiate a litigation hold. If you do wait to see what happens, you should probably expect a claim of spoliation of evidence somewhere along the line.

eDiscovery does not just affect litigators. Planning for and dealing with eDiscovery is part and parcel of any good corporate, employment, public sector, private sector, or any other type of legal practice where you offer ongoing client advice. If you are not a litigator and think you can ignore this burgeoning area of the law, you might as well put your malpractice carrier on notice now.

In fact, a new breed of eDiscovery advice lawyer is beginning to emerge. That lawyer blends a thorough knowledge of the litigation process with knowledge about electronic records management, general records management, industry specific regulatory compliance, and comprehensive IT knowledge about hardware, software, email, Internet usage, networks, storage devices, and the many other technologies that are now part of our normal day to day business operations.

Planning for and dealing with eDiscovery is part and parcel of any type of legal practice where you offer ongoing client advice.

This article focuses on the first step in George Socha and Tom Gelbmann's landmark [Electronic Discovery Reference Model \(EDRM\)](#): Information or Records Management. Next week, I'll discuss the Identification and Preservation phases.

WRITTEN RETENTION/DESTRUCTION POLICIES

eDiscovery lawyers should get involved in the creation and implementation of document retention and destruction policies. A written policy to manage both paper and electronic information is a must. Furthermore, the policy when written must be followed, and mechanisms must be put in place to ensure compliance.

(Continued on next page)

If done, you are more likely able to rely on the “safe harbor” provisions of Rule 37 when information is inadvertently destroyed as part of the routine, good-faith operation of a client’s electronic information systems. Regular compliance with a standardized written destruction policy is far more likely to persuade a judge not to order sanctions for the destruction of information destroyed prior to the institution of a litigation hold.

The benefits of a proper retention/destruction policy include:

- Making sure that all critical legal and business records are retained for the appropriate time period.
- Making sure that any regulatory or legislative requirements are met (e.g., Sarbanes-Oxley, HIPAA, Gramm-Leach Bliley, FACTA Disposal Rules, etc.).
- Making sure records are maintained in the proper format, especially in native format for electronic documents where preservation of metadata may be an issue.
- Avoiding claims of spoliation of evidence.
- Early identification and preservation of privileged information.
- Cost containment of eDiscovery related costs.

Email is by far the biggest component of any enterprise’s ESI, and it is typically the most fruitful area when searching for useful evidence in litigation.

Any such policy must conform to the needs and practices of the organization. It necessarily involves consultation between legal counsel, records management, and IT personnel. It is also very useful to obtain executive level approval of such plans. Making sure key decision makers understand the exposure risk if this important issue is ignored, and the benefits of being prepared, will help them un-

derstand and approve any non-standard expenses incurred in implementing a plan.

Too often IT or records management personnel submit a valid proposal at budget time requesting new software, hardware, or related expenditures to implement such a policy. At first blush, uninformed senior management may see these expenses as unnecessary and easy to eliminate. They need help, however, in understanding why they are being penny wise and pound foolish.

EMAIL RETENTION SYSTEMS AND POLICIES

Even if a company is reluctant to create an enterprise-wide retention/destruction policy, special consideration should be given to the development of a proper email management plan. Email is by far the biggest component of any enterprise’s ESI, and it is typically the most fruitful area when searching for useful evidence in litigation.

In the past, too many companies have relied on backup tapes to serve as their email archive. Doing so results in significant restoration and review costs if eDiscovery becomes necessary.

The current trend is to use email filtering and archiving programs, and to develop written procedures for the use of such systems. These technologies ensure that pertinent information is saved in an archive that is searchable by user, recipient, date range, key words, or other search parameters that can rapidly and cost-effectively retrieve relevant information.

DEDUPLICATION

Another component of a good records management plan deals with the management of duplicate information. Every time an email goes out say to twenty recipients, along with multiple attachments, the space needed to store the duplicative information grows enormously. To reduce the storage requirements a company may want to implement a plan that includes some or all of the following:

- Automatic destruction of duplicates after the master document has been retained in a document management system.

(Continued on next page)

- Use of shared folders with links to files included in email rather than attaching copies of the documents to email.
- Creation of a policy to require destruction of drafts so only the final version is maintained.
- Creation of a policy that designates the sender or the recipient as the person responsible for saving the document or email.
- Establishment of mailbox size limits and purge policies for information that is not otherwise saved in a document management system.

METADATA PRESERVATION

It is now clear that metadata associated with a given electronic file must be preserved and is potentially discoverable. While this information is often superfluous, it may contain the “smoking gun.”

Metadata associated with email includes headers, attachments, date and time, domain names, and recipient lists. Metadata in system files can provide information about revisions, modifications, creation dates, file size, authors, etc. If you use Microsoft Word it includes Track Changes information, and if you use Excel it includes unseen formulas and other hidden information. Obviously, when dealing with ESI there is much more than meets the eye.

Whether in the end the metadata will need to be produced in discovery is a concern that arises later in the process. At the time the duty to preserve arises, and the institution of a litigation hold is required, steps must be taken to preserve metadata. Some companies use metadata strippers as part of their daily IT process. While there is nothing wrong with stripping metadata from email and its attachments, or even when the final document is saved to an archival file, once the reasonable expectation of litigation arises steps must be taken to suspend the use of such technology. When litigation begins, and a meet and confer is in order, one of the important issues to deal with at the outset is the extent to which you need to engage in ongoing efforts to preserve metadata. It can be expensive and disruptive to do so, and in the real world there are a very limited number of cases in which metadata is truly relevant to the issues in dispute.

Proper consideration of the type of metadata removal software to use and when to use it is required. As a trial lawyer I have no problem defending the stripping of metadata in email and its attachments. For example, we lawyers make sure that a document copied from one matter and then revised and saved for another matter is stripped of any information in Track Changes that might disclose confidential information unrelated to the matter at hand. The same concerns exist among your clients in the normal course of their respective businesses as well.

It is now clear that metadata associated with a given electronic file must be preserved and is potentially discoverable.

On the other hand, I look forward to the day when I can cross examine the IT director or management person who implemented a plan to strip metadata from every single document or spreadsheet that is saved on a company server. I suspect by the time I'm done a jury will assume that the company must be guilty of something, or has something quite nefarious to hide if it engages in this type of activity on a regular basis. The implications of defending such a practice are not always apparent to an IT manager or corporate official when they make the decision to implement such a plan. And that explains why legal, IT, and records management personnel must work together on this issue.

AUDITING

As mentioned above, a key component to a successful records management is the ability to enforce and prove compliance. You should periodically audit and document compliance at both the user end and at the IT end since it's not uncommon for lapses to occur at both ends of the process. Corrective measures should be taken where needed and also documented. Mistakes can happen, but the point of this effort is to establish a good faith effort to properly manage a company's records.

(Continued on next page)

Auditing should also include a periodic review of the policy itself. In this rapidly-changing area, what may be an appropriate practice today may suddenly not be appropriate when a new technology becomes available for document management and review, or a change in the company's operations requires an overhaul of its policy and practices.

... to be continued.

Copyright 2008 Bruce A. Olson. All rights reserved.

ABOUT THE AUTHOR

Bruce A. Olson, is a shareholder in the Milwaukee based law firm of [Davis & Kuelthau, S.C.](#) A trial attorney and nationally recognized legal technologist

focusing primarily on the areas of electronic discovery and litigation technology, Olson is AV rated and Board Certified by the National Board of Trial Advocacy. He is co-author of "The Electronic Evidence and Discovery Handbook: Forms, Checklists and Guidelines," published by the American Bar Association. He received the prestigious "Techno-Lawyer of the Year 2002", from the TechnoLawyer Community, and was Chair of ABA TECHSHOW 2004, Vice Chair of ABA TECHSHOW 2003, and served on the TECHSHOW Board of Directors from 2000-2004.

Contact Bruce:

E: bolson@dkattorneys.com

T: (920) 431-2230

About TechnoFeature

Published on Tuesdays, *TechnoFeature* is a weekly newsletter containing in-depth articles written by leading legal technology and practice management experts, many of whom have become "household names" in the legal profession. Most of these articles are TechnoLawyer exclusives, but we also scour regional legal publications for superb articles that you probably missed the first time around.