



Electronic Dispatch

Labor and Employment Law Information Memo

November 2004

[Go to BS&K Labor and Employment Law Home Page](#)

DISCOVERY AND RETENTION OF ELECTRONIC FILES IN EMPLOYMENT LITIGATION

Parties to either pending or *foreseeable* litigation have an obligation to preserve all evidence in their possession that may be relevant to that litigation. In the context of employment litigation, a statement by an employee or former employee indicating an intent to file a discrimination charge with a state or federal agency may be sufficient to trigger this obligation to retain all personnel records relating to that individual, all communications between the company and that individual, and all other records relating to that individual's employment.

The obligation to preserve evidence applies not only to paper documents, but also to documents stored on an employer's computer system, such as e-mail messages, word processing files, Excel spreadsheets, PowerPoint presentations, voice mail and other electronic data. The obligation may even extend to information stored on a key player's personal computer, "Blackberry™", or other PDA. Because an employer's failure to meet this obligation can result in severe court-imposed sanctions, it is important for all employers to maintain and follow a document retention policy for both paper and electronic documents.

This Information Memo describes the adverse consequences that can result from an employer's failure to retain electronic files in the face of actual or threatened litigation, and sets forth some of the features of an effective document retention policy.

Court-Imposed Sanctions for Spoliation

Spoliation is defined by the federal courts in New York as "the destruction or significant alteration of evidence, or the *failure to preserve property* for another's use as evidence in pending or reasonably foreseeable litigation." If a court determines that spoliation has occurred, it has the discretion to impose a variety of sanctions upon the party that failed to preserve evidence. Among other sanctions, a court may: (1) require the payment of attorneys' fees and costs incurred by the opposing party resulting from the spoliation; (2) draw an adverse inference that the evidence that was not preserved would have been unfavorable to the party that failed to preserve it, thereby providing a basis to deny summary judgment; (3) instruct a jury that it also can draw an adverse inference from the failure to preserve evidence, thereby allowing an unfavorable verdict; (4) preclude a party from introducing its own evidence related to the information that was not preserved; and (5) even order default or dismissal.

A recent decision of the United States District Court for the Southern District of New York, [Zubulake v. UBS Warburg LLC](#), demonstrates the adverse consequences that can result from an employer's failure to preserve electronic files in the face of actual or threatened employment discrimination litigation. In [Zubulake](#), the plaintiff filed a sex discrimination charge with the Equal Employment Opportunity Commission on August 16, 2001. However, the court found that the employer's duty to preserve relevant documents arose in April of 2001, when key players in the Company by their own admission first began to fear that litigation could arise in the future. The court also found that the employer's personnel had deleted and/or failed to preserve relevant e-mail messages after that April obligation to preserve relevant documents arose. As a remedy for the employer's conduct, the court ordered that the jury would be allowed to draw an inference that the deleted e-mail messages were favorable to the plaintiff and unfavorable to the employer. The court also ordered the employer to pay the plaintiff for any attorneys' fees and costs that would be incurred if further depositions were necessary to seek evidence from alternative sources as a result of the deletion of the e-mail messages.



Document Retention and Destruction Policies

The increasing prevalence of e-mail as the primary method of business communication and the decreasing propensity to maintain paper copies of documents stored in a computer system have made it more difficult for employers to meet their obligation to preserve records in the face of actual or threatened litigation. Employers that maintain and follow an effective document retention policy will be in a better position to defend themselves against employment claims, and will reduce the risk of a spoliation finding.

At its most basic, a document retention policy describes what records (both paper and electronic) should be saved, where they should be saved, in what format, and for how long. It also sets out the company's requirements regarding document destruction. As a starting point for developing a document retention policy, a business should evaluate the types of documents it generates and receives. The various types of documents can then be categorized into related groups based on the length of time those documents will remain useful to the business. The policy should provide for destruction of various types of documents only after they have outlived their business usefulness or any applicable statutory periods. For example, certain types of documents may be designated for permanent storage, while other types of documents may be designated for destruction after a specified time period following creation.

A document retention policy should not only specify how long different types of documents should be retained, it should also specify how those documents will be destroyed and who will be responsible for destroying them once the retention period expires. For example, a company's Human Resources Manager may be designated as the individual responsible for overseeing destruction of personnel documents after they are no longer useful, while a company's Chief Financial Officer may be responsible for overseeing the destruction of financial records after they are no longer useful.

Many companies have software programs that automatically delete electronic files from a computer system after a certain specified period of time as part of their document retention policy. Although these types of software programs can be extremely useful in streamlining the amount of information on a computer system, companies should examine the type of information that is automatically deleted and the length of time that the information remains on the system to ensure that relevant information is not automatically destroyed. Employees should be informed that they are responsible for determining what information should be shielded from automatic deletion and should be trained with respect to how to save that information to other files in order to prevent automatic deletion.

"Litigation Hold" Provisions

In addition, a document retention policy must have a quick and effective method of suspending any automatic deletion aspects once the employer becomes aware of actual or threatened litigation. A company's failure to halt the routine destruction of documents, whether pursuant to a paper document destruction policy or due to automatic deletion of electronic documents, can result in the sanctions for spoliation described earlier. In other words, the fact that information was destroyed inadvertently due to an automatic deletion system will not shield an employer from responsibility.

Accordingly, once a company becomes aware of actual or threatened litigation, it should identify the individuals who are likely to have generated or received information relevant to the matter and should notify those individuals that all documents (both paper and electronic) must be preserved. The company's information technology department should also be immediately notified so that any automatic deletion of electronic documents relevant to the matter can be suspended.

An effective document retention policy, including "litigation hold" provisions, should cover business records and communications maintained by employees on their home computers, laptops, and other electronic devices as well. Employees should be informed that they are responsible for preserving such files for the period of time specified in the document retention policy and/or transferring those files to the company's computer system, and that disciplinary action can result from their failure to comply with the document retention policy.

To effectively implement a document retention policy as it applies to electronic documents, a company should designate an individual (for example, an Information Technology Manager) to oversee the retention and destruction of electronic information. This individual should have a thorough understanding of how the electronic system works, how to categorize and search for information within the electronic system, and how to evaluate the company's record retention needs in light of its business goals and legal obligations. A company should also distribute its document retention policy to its employees, and train its employees with respect to the retention of paper and electronic files.

If you have any questions regarding your obligation to preserve records or would like assistance drafting a document retention and destruction policy, please contact:

In the Capital District, call 518-533-3000 or e-mail:

John M. Bagyi jbagyi@bsk.com Nicholas J. D'Ambrosio ndambrosio@bsk.com

In Central New York, call 315-218-8000 or e-mail:

R. Daniel Bordoni dbordoni@bsk.com Robert A. LaBerge rlaberge@bsk.com

On Long Island, call 516-267-6300 or e-mail:

Terry O'Neil toneil@bsk.com

In New York City, call 646-253-2300 or e-mail:

Michael I. Bernstein mbernstein@bsk.com Louis P. DiLorenzo ldilorenzo@bsk.com
Stanley Schair sschair@bsk.com

In Western New York, call 716-566-2800 or e-mail:

Robert A. Doren rdoren@bsk.com Daniel P. Forsyth dforsyth@bsk.com
Richard C. Heffern rheffern@bsk.com

