How to Win the Battle Over Electronic Discovery in Employment Cases

By Philip L. Gordon, Esq.

LITTLER MENDELSON, P.C.
THE NATIONAL EMPLOYMENT & LABOR LAW FIRM®

IMPORTANT NOTICE

This publication is not a do-it-yourself guide to resolving employment disputes or handling employment litigation. Nonetheless, employers involved in ongoing disputes and litigation will find the information extremely useful in understanding the issues raised and their legal context. This white paper is not a substitute for experienced legal counsel and does not provide legal advice or attempt to address the numerous factual issues which inevitably arise in any employment-related dispute.

How to Win the Battle Over Electronic Discovery in Employment Cases

By Philip L. Gordon, Esq.

More than almost any other type of lawsuit, employment cases provide plaintiff's counsel with the opportunity to use "electronic discovery" – in particular, requests to produce word processing documents, electronic mail and instant messages, spreadsheets, etc. – to force employers into submission. In virtually all employment cases (with the exception of trade secrets cases), electronic discovery is a one-way street; the employer controls the electronic resources of most witnesses, including the plaintiff; possesses most of the relevant electronic records; and may not even be able to contend legitimately that plaintiff's personal computer is a valid target of discovery. In contrast to commercial litigation involving tens or hundreds of millions of dollars, the cost of responding to requests for electronic discovery in employment cases and the potential monetary sanctions for failing to do so – especially in single-plaintiff cases – can easily become disproportionate to the amount in controversy. And, an "adverse inference instruction," i.e., the judge's instruction that the jury may draw an inference that destroyed electronic files contained information adverse to the employer's case, easily could be the death knell for a defendant-employer already portrayed by plaintiff's counsel in opening statement and closing argument as the overbearing brute.

Employers can, however, prevent electronic discovery from becoming their adversary's silver bullet. As with any form of warfare, disarming the adversary's most effective weapons requires planning long in advance of the actual battle and crisp execution once the gauntlet has been dropped. In the battle over electronic discovery, employers can achieve these overarching objectives by taking the steps discussed below to the extent warranted by the nature of the dispute, the anticipated cost of litigation and the amount potentially in controversy.

Step 1: Develop & Implement a Reasonable Data Retention & Destruction Policy

Electronic discovery can easily become a bludgeon in the hands of plaintiff's counsel for three principal reasons. First, electronic records are stored in vast quantities on a wide range of storage media, including network and e-mail servers, workstations, laptops, personal digital assistants (PDAs) and portable storage media, such as CDs, UBS drives, and floppy disks. Consequently, searching for, retrieving, reviewing and producing electronic records can be very time consuming and costly. Second, retrieving electronic records from back-up tapes created for disaster recovery purposes can be exorbitantly expensive because this process often requires the services of data recovery specialists and the re-creation of the antiquated computer environment in which the data originally was created. Third, employees are in a position to eliminate electronic records from easily accessible storage media — whether intentionally or accidentally – thereby making the employer vulnerable to charges of spoliating evidence and making it more likely that a court will sanction the employer and/or order the employer to spend substantial sums to recover the otherwise easily retrievable data from back-up tapes.

Employers can significantly mitigate each of the three factors that make electronic discovery an effective weapon in the hands of aggressive plaintiff's counsel by developing and implementing a data destruction and retention policy. Electronic records destroyed in accordance with such a policy obviously are unavailable to be produced, reducing the cost of searching for documents, reviewing them for relevance, privilege, and trade secrets and ultimately producing them. As long as the records destruction policy was implemented before litigation was on the horizon, establishes reasonable and legitimate guidelines for data destruction, and is uniformly enforced, courts generally will not sanction employers that have followed the policy and destroyed electronics records that would have been discoverable had they existed when the employer first received notice of the litigation.

Step 2: Promptly Inform Employees of the "Litigation Hold"

An organization becomes subject to a duty to preserve potentially discoverable information when it knows, or reasonably

should know, that the information might be discoverable in litigation. In the employment context, the duty attaches, at a minimum, when the employer is served with notice that a formal proceeding has commenced – for example, by service of a complaint or receipt of a charge of discrimination or other notice that a government agency will be conducting an investigation. The duty can be triggered even before a formal proceeding is commenced, most commonly when an employee's attorney sends a demand letter, even if the letter does not include a demand to preserve evidence. Litigation counsel should be consulted as soon as the duty to preserve is triggered, or even when it is unclear whether the duty has been triggered.

When the duty to preserve evidence does attach, the organization must implement a "litigation hold." The "litigation hold" entails (a) an immediate suspension of any routine practice, policy or procedure of destroying any documents or data that are potentially relevant (including electronically stored records, such as email and instant messages); and (b) collection and preservation of such documents/data for use in the litigation. Given the ease with which electronic records can be deleted, discarded or overwritten, implementing an effective litigation hold requires detailed instructions to employee-witnesses, records-management personnel, and information technology (IT) staff.

These employees should promptly be sent a memorandum that achieves the following:

- Informs them that the organization is under a duty to preserve relevant evidence, including both paper documents and those that are stored electronically and that all document destruction in accordance with organizational policy must be suspended.
- Explain that the litigation hold applies to information on the company's network servers, e-mail server, workstations, laptops, portable hard drives, PDAs, employee personal computers and all other storage media, such as diskettes and CDs, as well as to all file types, including e-mail, word processing documents, spreadsheets and power point presentations.
- Identify the categories of documents that must be preserved and the time frame encompassed by the litigation hold.
- Explain that failure to comply with the instructions could result in discipline for the employee and the imposition of sanctions on the organization.

The IT Department should receive additional instructions. These include the following:

- Disable any computer programs that automatically destroy potentially relevant evidence, such as e-mail and instant messages.
- Remove from the recycling routine any accessible back-up media (i.e., back-up media from which data can be easily retrieved without a restoration process) for the relevant time period.
- If it would not be unduly burdensome, store the hard drives of the computers used by employees likely to be key players in the litigation until it can be determined whether it would be cost prohibitive to create a mirror image of those hard drives.
- Do not discard or re-issue any computers used by a departing employee likely to be a key player in the litigation.

Step 3: Consult with Litigation Counsel Concerning Electronic Discovery

Litigation counsel will need to work with the organization's personnel — typically, in-house counsel, IT personnel, and records management specialists — to gather discoverable records. Before that process can get started, in-house counsel will need to identify for litigation counsel (a) the employees who likely will be key players in the actual or impending litigation, (b) the individuals in the IT and records management departments who will serve as "point persons" for litigation counsel, (c) the pertinent time frame for the matter in dispute, and (d) the categories of potentially discoverable electronic data/documents.

IT staff will need to educate litigation counsel about:

- the nature of the organization's electronic storage systems;
- the computer resources available to, and used by, the key players; and
- where the electronic data (including e-mails and instant messages) and other potentially relevant documents generated or received by them may be found (i.e., network servers, e-mail servers, workstations, laptops, PDAs, home computers used for business purposes, etc.).

Litigation counsel will also need to know the following:

- whether the client's systems automatically purge certain electronic records, such as e-mail stored in an in-box after a predetermined time after receipt;
- whether deleted items (particularly e-mail) can be easily restored through the use of the "restore delete" function;

- whether IT staff routinely recycles back-up tapes and, if so, on what schedule;
- whether the client ever uses its back-up tapes as a means of archival storage or if such tapes are accessed only for disaster recovery purposes;
- whether the client had disposed of or recycled any computers or storage media used by the key players; and
- how the client handles data stored on computers used by departing employees.

Step 4: Provide Litigation Counsel with Information About the Organization's IT Resources

Litigation counsel will be better able to respond to, and defend against, the adversary's electronic discovery requests when armed with an understanding of the organization's electronic resources. Having this information also will place counsel in a better position when interviewing key players to understand their "electronic habits." In addition, this information will be important for technical consultants — litigation support and forensic experts — when they evaluate the best methods for gathering and preserving discoverable documents.

With reference to the parameters of the litigation hold, the subject matter of the actual or threatened litigation, and the ultimate objective of locating and preserving potentially discoverable electronic information, the specific information to gather for litigation counsel typically will include the following in most employment disputes involving electronic discovery:

Policies and Procedures. Provide written policies concerning the organization's computer resources, including data retention and destruction policies, back-up recycling schedules, e-mail use and retention policies, computer use policies, telecommuting policies, and password, encryption, and other security protocols.

Company-Issued Devices Used By Employees: Provide the brand name, model number, and serial number of each company-issued device (work stations, laptops, PDAs, etc.) used by each key player during the relevant time period.

Storage Media: Identify all locations where active files are maintained, including, for example, network servers, e-mail servers, local hard drives, laptops and diskettes. Identify storage likely to contain duplicative data. Provide a description of labeling standards and storage procedures for CDs and diskettes.

E-mail: Provide the type of hardware (servers and terminal devices) and software used during the relevant time period, including each version of software; the number of users; the location of mail files; password usage; and whether employees use off-site e-mail services from work and, if so, whether these are corporate or personal accounts. If the organization has an enterprise instant messaging (IM) system, provide similar details for that system. If the organization does not have enterprise IM, determine whether any of the key players used IM at work and discuss with IT staff (and forensic experts) the possibility of recovering instant messages.

Document Destruction: Explain how electronic and paper documents are destroyed and how the organization documents the destruction. If any potentially discoverable categories of documents already have been destroyed, provide any documentation of the destruction and identify the person(s) who destroyed the documents. If IT staff or records management personnel are aware of any material deviation from the policy with respect to any category of potentially discoverable information, provide information concerning the deviation.

In cases where electronic records will be central to resolving the dispute, or where plaintiff's counsel has signaled an intention to engage in aggressive electronic discovery – for example, by demanding preservation of substantial quantities of electronic records — the employer also should encourage IT staff and records-management personnel to collect the following information for litigation counsel:

Personnel: Create, if one does not already exist, an organizational chart that identifies IT and records management positions, ideally including those employees responsible for system maintenance, electronic mail and instant messages, electronic records management and data destruction.

Security Measures: Certain security measures, such as activity logs, audit trails, and monitoring software may be the source of useful evidence. For example, network resources that log user activity can be used to prove that a departing employee accessed sensitive data immediately before going to work for a competitor.

Back-Up Storage: Provide the brand name and version of back-up software and back-up drives; the type of storage media used and the storage capacity; back-up procedures and schedules including non-routine back-ups (for example, Y2K or before a system upgrade); the schedules for maintaining and recycling back-up media; and how back-up media are indexed, stored, and retrieved, both on- and off-site. If the organization changed or

upgraded hardware, operating systems or applications software during the relevant time period, provide the brand name and version of any replaced hardware, operating system or application software that will be needed to restore back-up data and determine whether "legacy" hardware and software and related user guides have been retained.

Application Software and Utilities: Provide the brand name and version of applications software and utilities used during the relevant time period, including both commercially available and custom applications, (e.g., programs for scheduling, project management, accounting, word processing, database management and encryption). Explain how shared files are structured and named on the system.

System Configuration: Provide the brand name and model of network servers, storage devices and workstations used during the relevant time period and an explanation of how the devices were configured.

Operating Systems: Provide the brand name and version of network and desktop operating systems used during the relevant time period.

Step 5: Make the Key Players Available for Interviews By Litigation Counsel

Litigation counsel should meet with each of the employees who likely will be a key player in the litigation. At this meeting, litigation counsel will remind each key player of the scope and meaning of the litigation hold and the potentially grave consequences of ignoring it. Counsel will work with each key player to identify the pre-existing records that must be preserved and records that might be created in the future that will need to be preserved as well. The information obtained by counsel from IT staff and records-management personnel can prove extremely helpful when litigation counsel tries to uncover potentially useful evidence through these interviews.

Step 6: Gather and Preserve Discoverable Information

The administrative exhaustion requirement applicable to many employment cases could result in a substantial lag between the time that the duty to preserve attaches and the time that discovery in a judicial proceeding commences. Preserving potentially discoverable information during this time period will require coordination among litigation counsel, the organization's lead IT contact, and the litigation support team. The ultimate goal is to create a "battle-ready" database that will permit litigation counsel to respond to discovery efficiently and at the lowest possible cost while providing an invaluable resource for defending the lawsuit.

Those involved in the data-collection and preservation process should discuss the following points:

Format and Method of Preserving Active Files: Active files can be preserved in native format or as images. Each format has advantages and disadvantages that should be considered. In addition, documents can be preserved on removable media (CDs and diskettes) or on servers that permit Internet-based access. Choosing among these options will depend upon the quantity and type of electronic data, the location of members on the litigation team and other factors. After selecting the format and method for preserving active files, the litigation team should identify each device and all other storage media from which data will be collected and develop a plan and schedule for the data collection process.

Back-Up Tapes: Restoring back-up tapes can be very costly and, in most circumstances, should be considered only in the context of responding to discovery specifically requesting the production of data on back-up tapes. At this stage of the process, the litigation team should focus its efforts on determining whether removal of back-up tapes from routine recycling is required and, if so, ensuring that (a) back-up tapes potentially containing discoverable information are located, indexed and removed from the recycling process; and (b) newly created back-up tapes potentially containing discoverable information are preserved.

Legacy Hardware and Software: If, during the relevant time period, the employer has changed or upgraded the hardware or software used to create back-up tapes, the employer should preserve legacy (or outdated) hardware and software and related user guides in the event the employer is ordered to restore back-up tapes created before the change or the upgrade.

Residual Data: Residual data, which encompasses deleted files, remains on a computer's hard drive until overwritten. To preserve residual data, a computer's hard drive should be imaged, a process typically conducted by a computer forensic expert. This process can be costly. The employer generally should await formal discovery before imaging any hard drives. Consequently, the litigation team should discuss taking the hard drives in question out of circulation so that residual data is not overwritten.

Chain of Custody: Keeping in mind that electronic records could

be favorable to the employer, the litigation team should ensure that it gathers and preserves evidence in a manner that will insulate the records from attacks on their authenticity. The litigation team, therefore, should focus on the technical steps that need to be taken to create an unassailable chain of custody. The employer's IT staff who are helping to gather information should be provided forms that permit them to record the categories of files that have been copied, the date and time of the copying, the identification of the storage media to which they were copied and the litigation attorney to whom the storage media were provided.

Cost and Administrative Burden: The litigation team should document the cost of gathering, preserving and producing electronic evidence and the administrative burden that those efforts impose on the employer's business. Litigation counsel will be able to use this information, when seeking a protective order or opposing a motion to compel, to carry its burden to prove that production is unduly burdensome. Courts typically require a fact-specific showing to meet that burden.

Once these topics have been thoroughly considered, the process of gathering and preserving electronic documents should be completed. If the employer and the key players will generate discoverable information after this process has been completed, or if new employees with access to potentially discoverable information will be hired, the organization must send periodic reminders concerning the scope of the litigation hold and the importance of not violating it.

Conclusion

While the specific details of planning and executing an organization's responses to electronic discovery requests will vary depending upon the nature of the organization and its internal resources, the nature and scope of the parties' dispute, and many other factors, the steps outlined above should provide a useful road map for most organizations. Following the road map should permit the employer to resolve litigation based on its merits rather than on avoiding the cost of electronic discovery and the imposition of discovery sanctions.