

# An E-Call To Arms

A Proactive Defense For Electronic Data Requests.

By Gene Klimov



LITIGATION CONSULTING

Lynbrook ■ New York City ■ Washington D.C. ■ 1-800-875-8705 ■ Fax 516-823-4400

[www.DOAR.com](http://www.DOAR.com)

Attorneys routinely face the obligation to produce relevant information in every litigation matter. Now that this information is increasingly in electronic form, electronic evidence has become a predominant topic of concern for both corporate executives and attorneys alike. In light of the penalties, severe sanctions and evidentiary misconduct actions issued by more judges within recent months, corporate counsel and defense attorneys are taking a closer look at just what it takes to produce this type of evidence. The manner in which this data is located, prepared and reviewed can present a daunting challenge. Understanding the characteristics of electronic data and the process involved in managing and producing it should help.

### Understanding the Differences

There are inherent differences in the way digital documents are created, stored and managed versus their paper counterparts. Electronic data has the unique distinction of being dynamic. Underlying data stored with every electronic file can be inadvertently altered simply by moving, copying or opening it. When responding to a request, everything from operating system specifications, application settings and header information to network storage, backup routines and management systems may come into play.

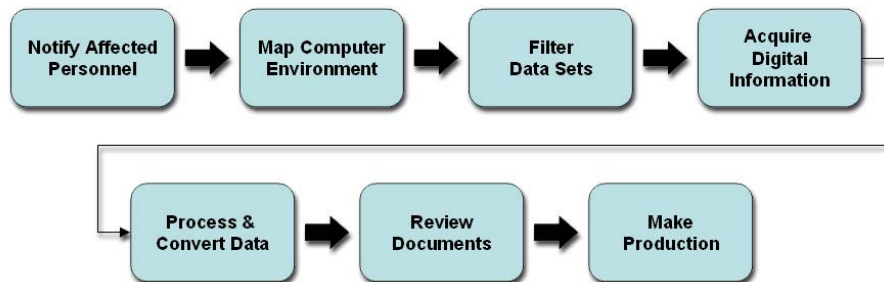
When storing paper documents, there is a physical limitation on the number of pages that can fit into a folder or file cabinet. However, when electronic files are stored, compression programs and archival software allow 2-5 times the amount of information to be stored within a given space. It is this ambiguity that plagues litigators in firms across the country in their ability to accurately estimate the amount of information that can be yielded from a given set of data (no matter how many industry averages for file size are used). Everything from file type, margin setting and pagination, hidden information and version tracking will affect the end result. Therefore, the more knowledgeable legal professionals become about the proper ways to work with electronic files and the realistic expectations necessary for understanding the scope of work, the less frustrating the situation will be.

### Preparing Your Response

When responding to a request for electronic data, making the right decisions at the onset of discovery are vital to ensuring a controlled and accurate production. IT staff can be invaluable in executing normal business operations and internal procedures. However, when it comes to making a decision about how to collect certain information for the purpose of review and ultimately production, you'll need more than technical expertise. There are a variety of factors that come into play when preparing data for delivery. For example, if a review is performed in a native environment that contains both application files and e-mails, there should be an electronic reference established for all original documents. By including review fields in this reference, hours spent by attorneys categorizing documents can be preserved and subsets easily created. Another factor to consider is whether to normalize the data by converting each document into a common format. This allows the information to be encapsulated to prevent unwanted alteration of data, converted from disparate versions of applications, and stored in such a way that all references to originating locations are preserved. As a result, when the review is conducted, the appropriate data is easily sorted and made available for production.

### Road to Production

Taking on a massive electronic data production project can be an overwhelming task filled with uncertainty and stress. Knowing the appropriate actions to take and especially when to take them could be the determining factor between a job well done and potential sanctions due to an inability to provide data to the requesting party. The following chart provides a framework to help organize and focus the collection and review process for the production of information.



### Notify Personnel

When the determination is made that a litigation or investigation matter is pending, the obligation to preserve any and all related information should be communicated throughout the organization. Every employee that may be affected by the imminent action should be made aware of the situation and educated on the type of information and subject matter that would potentially apply to the preservation order. Create a procedure by which individuals can adhere to the obligation without interfering too much with day to day work and organizational obligations. If a procedure is premature, specify temporary actions that individuals can take and identify a time period when a more formal plan will be put in place.

### Map Environment

In responding to a request for data, it is important to understand the layout and interaction of the client's systems that apply to the request. The best way to approach this daunting task is to meet with the heads of each area and document the vital information. The information collected will allow you to map out the important areas of operations and how they interact with each other. Critical systems will most definitely include centralized e-mail systems, database tracking systems for clients, products or institutional knowledge, accounting and financial systems, archival and disaster recovery. In addition to these components, there are supporting systems that may appear to be free from relevant data on first inspection, but often times contain valuable information. For example, fax servers sometimes save copies of all transmissions in and out of an organization, anti-virus applications allow logging of every file that passes through the network and other systems like proxy servers often retain internet traffic and e-mail forwarding information. Keep in mind that other systems may contain relevant data and the best way to uncover it is through the administrators and users in the respective departments. Aside from the central systems, get a sense of the user environments to determine if data can be stored locally, hosted on an ASP or even transferred off site for remote access. With today's synchronization

technology, employees can take all sorts of information from the office, so be forewarned. As you build the information collection, construct a list of every employee that is affected by the request. Identify information that each user has access to in addition to potential areas of stored data.

#### Filter Data

The responsibility of determining what is or is not relevant to discovery demands falls on the producing party. Obligations should be identified and defined to limit the scope to relevant information and avoid undue burden and cost. This is typically done by including the information accessed by specific individuals rather than searching through corporate-wide systems.

#### Acquire Data

At this point, the relevant information that has been identified and filtered should be more than sufficient to begin the collection process. Systems administrators, under the guidance of counsel, should create copies of information that is stored on file servers. Typically, user's e-mail accounts are stored centrally and the creation of an exact portable copy should be a straight forward process. User data may also exist in designated folders on network file servers so careful consideration of those locations should also be made. When preserving electronic files, it is important to remember that copying information for the purpose of creating data sets may inadvertently change the file system properties for those files. Special copy routines or archiving software should be utilized to ensure the authentication of these properties and attributes. In some cases, it may be necessary to invest in the services of a third party to document and testify to the collection process.

In some circumstances, it may be necessary to forensically image data so that further investigation can take place. For example, if there is a possibility that information resides in the form of deleted files or fragments of temporary memory, you may need to create bit by bit copies of user stations at a later point in the litigation process. Images that are created early on in the process will illustrate the proactive measures taken to ensure the preservation of the data. These situations are not common, but usually prove costly if the files become important later on. In addition to creating images of user systems, it may be necessary to collect a full set of backup tapes for the network servers and to preserve tapes on an ongoing basis. This would be determined at the onset of the case due to the fact that the costs associated with such preservation methods often meet or even exceed the amount in dispute.

#### Process & Convert

Before the data is prepared for review, every document is accessed and vital metadata is extracted. Each piece of information is saved in a central database for sorting, searching and use in the review process later on. After this database of information is created, there are several options available that will alleviate the burden of reviewing so many documents. The first and sometimes controversial option is de-duplication. This is the process of removing exact duplicates from a given population by first generating a unique identifier based on information going down to the bit level. That is, if two identical documents have one character changed, the unique identifier will be completely changed indicating that it is

not a duplicate. Then, all of the assigned values for every document in a collection are compared to identify the duplicates and potentially remove them from the universe of documents. The industry average tends to lie between 20% - 30% of duplication when dealing with archived sets spanning several years. There are many methods available in the industry to assign this unique value so it is important to understand the particulars before proceeding with this as a viable option. The second option to narrow the scope of relevant information is to define a set of terms to be used as search criteria across the collection. This usually involves a consensus from all parties to ensure that the terms are not too specific or overly broad. Once these terms are established, the scope of information can be significantly reduced.

Now that the data has been culled, de-duplicated and searched, it is converted into a single format, unusually TIFF or PDF, to facilitate an efficient review. Conversion removes the need for native applications to be installed, avoids potential problems with viruses embedded in the documents and keeps the file formatting intact. There may be some formats that will require the use of native applications for accuracy such as database files, dynamically linked web pages or complex spreadsheets that reference data from many locations. Nevertheless, conversion should allow for the specification of formatting and pagination from the native application for commonly used business applications. Whether it pertains to revealing columns in spreadsheets or exposing the changes tracked in word processing documents, it is important to know that these settings may limit the amount of information displayed or extend the number of pages to considerable quantities.

#### Review the Documents

After conversion, it is common to inspect every document for privileged information, trade secrets or even relevancy. One of the methods available for reviewing these converted documents is to print out the images to paper along with the metadata information of where the document came from or when it was created. Another method is to import the converted data into an in-house litigation support system. There are many popular applications available that allow for the import of a database filled with the information extracted during the conversion process in addition to linking each document record to a corresponding image. These systems allow attorneys to establish categories or classifications that documents can be placed in so after a review is completed, entire categories of documents can easily be accessed for further review or production. Lastly, all of the information as well as the images can be hosted on a secure web based repository. This eliminates the cost of high end internal systems and allows multiple parties to access the same information from any location with an Internet connection. These sites provide complex searching and retrieval, coding of information and the creation of production sets for purposes of print or delivery to opposing counsel. Think of it as a supply chain of information that can be accessed and shared by all members of the trial team and/or all outside counsel

#### Make the Production

At this last stage of the process, the creation of production sets in any form is relatively simple. The data now exists in a structured environment with all documents referenced back to the originals. Attorneys can choose to produce in paper form, electronic media or

remotely via a web based repository. The entire process boils down to this last step with special care taken to ensure consistency, the creation and management of production sets should be hassle free.

## Conclusion

Any production request can seem like an impossible undertaking that would require unlimited resources, both physical and financial. Without the proper understanding of industry options, tools and expert capabilities, this may not be far from the truth. It is the fiduciary responsibility of corporate and outside counsel to arm themselves with the knowledge necessary to make educated decisions about the way in which electronic evidence is collected and produced.