GIBSON DUNN

Vol. 1, No. 6

E-Discovery Basics: Preservation of ESI, Part 2

This is one in a series of brief introductory guides to practical issues in electronic discovery. To subscribe to future installments of E-Discovery Basics, please click here.

In our last installment of E-Discovery Basics, we discussed four general categories of electronically stored information ("ESI") that should be considered for preservation pursuant to a legal hold: active data, inactive and archived data, residual data, and legacy data. Here, we further discuss common sources of relevant ESI and certain common file types to consider preserving, collecting and reviewing.

The sources of relevant ESI and file types will, of course, depend on the issues in the case. An employment dispute, for example, will usually implicate different sources than an antitrust class action. While some sources may be considered in most cases (*e.g.*, e-mail accounts and servers), other sources may only be implicated in certain types of matters (*e.g.*, an accounting database or an external website). Ordinarily, the starting point for determining sources of ESI for preservation is to analyze the allegations or claims that triggered a duty to preserve and to identify key players and others who had any involvement in the issues. The next step, typically, is to determine how these custodians communicated, how they created and stored potentially relevant ESI, and what systems they used in doing so. IT and records management personnel should also be consulted about potentially relevant systems, backup, archiving and purging protocols, and document retention periods (which may need to be suspended to ensure that relevant ESI is not destroyed). The process will likely be iterative, with additional sources identified as more is learned about the matter. A data map and retention schedules can be very helpful in expediting this process, reducing the risk that relevant information will be lost, altered or destroyed.

Obviously, not every source of ESI and file type will be relevant in every matter. But it is important not to overlook potential sources of relevant information, which for better or worse are proliferating, resulting in additional challenges for those implementing legal holds. While not an exhaustive list, some common sources to consider for preservation include the following:

Communications: Email is often the central source of relevant ESI in litigation and investigations. It may reside on the custodian's laptop or desktop computer, PDAs such as BlackBerrys, the company's email servers, and in backups and archives (including storage provided by third-party vendors). Considering whether custodians had relevant communications in web-based email applications such as Google Gmail and Yahoo! Mail or external email systems such as Bloomberg Mail, and whether they

did so on home computers, may also be prudent. But other forms of communication are also prevalent and may also warrant consideration for preservation—instant messaging and chat, for example. IMs and chats can usually can be found in similar locations to email—*i.e.*, computers, PDAs, servers, backups and archives—and may also be on web-based and external systems such as AOL Instant Messenger, MSN Messenger, Yahoo! messenger, Instant Bloomberg and Thomson Reuters Messenger. Mobile phones and PDAs may contain emails, text messages, images and information regarding phone calls. It may be appropriate to consider whether ESI stored in a custodian's electronic fax system, or in a videoconferencing system, is available and should be preserved. And, in some situations, audio recordings may exist that should be considered for preservation.

Databases and Other Applications: ESI related to dynamic databases—*e.g.*, those built on Oracle, SAP, SQL Server, *etc.*—may be relevant in some cases. For example, an employment matter may involve ESI from a company's human resources system, an antitrust matter may involve customer relationship management, sales or production systems, and a financial fraud case may involve accounting and finance systems. Depending on the issues, a matter may involve a company's electronic document management systems (EDMS), electronic records management systems (ERMS), or collaborative tools. Some database applications automatically purge data after a particular time period, so it can be advisable to identify and suspend such processes if necessary. Additionally, legacy systems—*i.e.*, software or hardware that is outmoded or has become obsolete—may exist and their data considered for preservation.

Workstations, Laptop and Home Computers and Removable Media: Relevant ESI may also be present on custodians' desktop, laptop or home computers. Even if a company has network-based document management systems, employees may have also been given the ability to save documents on a local hard drive, such as in a "My Documents" folder. Additionally, although some companies have policies prohibiting employees from using non-work issued computers, it may be advisable in certain situations to confirm whether, for example, key custodians in fact complied with the policy. Custodians may also have copied documents onto removable storage media, such as thumb drives, external hard drives, DVDs or CDs.

Network Storage: Documents may be stored in various places on a company's internal network—for example, shared drives, network disk drives, and servers. Servers are central computers on a network holding ESI or applications that multiple users of the network share through their client computers. For example, there are Web servers that send out Web pages, mail servers that deliver email, list servers that administer mailing lists, FTP servers that hold FTP sites and deliver ESI to requesting users, and name servers that provide information about Internet host names. File servers provide storage for files on a network—*e.g.*, email, financial data, or word processing information.

Backup and Archives: It is common for companies to back up the ESI on their information systems onto tape or other media for disaster recovery purposes. Additionally, some companies retain certain communications and other documents—*e.g.*, email and instant messages—through journaling and archiving. Backup media and archives that contain unique copies of relevant data should be preserved, which may require freezing retention periods and suspending the rotation of backup media. Even if the information may also be available in the company's active files, a company may still wish to preserve backups and archives out of an abundance of caution.

Third-Party Vendors: Various third parties may have ESI that a company may be deemed to control (*e.g.*, by virtue of a contractual relationship) and consequently may fall within the company's preservation obligation. Many companies employ business service providers (*e.g.*, accounting, payroll, human resources), application service providers (ASPs) that provide software or computer based services over a network (known as Software as a Service or SaaS), and external backup and disaster recovery storage. Cloud storage—networked external data storage where data is stored on multiple virtual servers hosted by third parties—is also becoming increasingly common.

Common file types: A few of the many common file types that might need to be preserved include word processing files (*e.g.*, .docx, doc., .rtf, or .wpd); text files (*e.g*, .txt or .asc), presentation files (*e.g.*, .ppt, .pot or .pps); email and other Outlook-type application files (*e.g.*, .pst, .ost, .pab, or .nsf); database extracts or reports (*e.g.*, .csv or .rpt); image files (*e.g.*, .pdf, .tiff, .jpg); web files (*e.g.*, .html, .xml); compressed files (*e.g.*, .zip); and in some circumstances partial, deleted, fragmented or corrupted files, if relevant.

Some courts have implemented rules providing that certain types of ESI are generally not discoverable—*e.g.*, deleted, slack, fragmented, or unallocated data on hard drives; random access memory (RAM) and other ephemeral data; on-line access data such as temporary internet files, history, cache, and cookies; and data in metadata fields that are frequently updated automatically, such as last-opened dates—unless a party demonstrates that such information is relevant. Even where such rules are not in place, it can be beneficial to attempt to reach an agreement with litigation opponents or government investigators that such files do not need to be preserved.

In the next installment of E-Discovery Basics, we will discuss collection of ESI for processing and review.

Other installments in our E-Discovery Basics series are available ***here****.*

If you would like to subscribe to future installments of E-Discovery Basics, please ***click here.***

Lawyers in Gibson Dunn's Electronic Discovery and Information Law Practice Group can assist in implementing defensible and proportionate approaches at all stages of the e-discovery process. For further information, please contact the Gibson Dunn lawyer with whom you work or any of the following Chairs of the Electronic Discovery and Information Law Practice Group:

Gareth T. Evans - Practice Co-Chair, Los Angeles/Orange County (213-229-7734, gevans@gibsondunn.com)
Jennifer H. Rearden - Practice Co-Chair, New York (212-351-4057, jrearden@gibsondunn.com)
G. Charles Nierlich - Practice Co-Chair, San Francisco (415-393-8239, gnierlich@gibsondunn.com)
Farrah L. Pepper – Practice Vice-Chair, New York (212-351-2426, fpepper@gibsondunn.com)