GIBSON DUNN

Vol. 1, No. 3

E-Discovery Basics: Litigation Preparedness

This is the third 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.

The Boy Scout motto, "Be Prepared," has particular import for companies that are likely to deal with e-discovery. Being prepared can help mitigate costs and risks, ensure timely compliance with preservation obligations, and bolster defensibility. The high costs often associated with e-discovery can worsen if outside counsel or an e-discovery consultant is forced to perform key preliminary tasks—such as generating organizational charts and investigating system architecture—from scratch. As in medicine, an ounce of prevention is worth a pound of cure.

When litigation or an investigation is pending or anticipated, a company should preserve relevant electronically stored information ("ESI") and hard copy documents by subjecting them to a legal hold. Delays in effectively implementing a legal hold can result in spoliation—the destruction or alteration of relevant evidence—which, in turn, can lead to a range of possible evidentiary or monetary sanctions. Proactively preparing for litigation makes timely compliance with preservation obligations more manageable. Companies can improve their litigation prospects by taking steps to help ensure that their e-discovery practices will be found defensible by a court. One way to increase defensibility is by having in place a repeatable and consistent process.

Companies can consider taking the following steps to improve their preparedness for e-discovery:

Develop a Records Management Policy. If the company does not have a records management policy with associated retention schedules, it should consider creating one. A policy that is proactively created, implemented, and enforced will likely better serve the company in litigation than randomly evolved and haphazardly implemented practices. Considering both company-specific and industry-specific litigation history and trends may help to identify the parts of the organization that are most likely to be involved in future litigation and investigations and therefore may deserve more attention and resources in the pre-litigation planning process.

An effective records management policy should reduce the accumulation of unnecessary data, thereby improving a company's operational efficiency. Removing unnecessary data also may confer advantages that are specific to litigation—*e.g.*, making compliance with discovery requests less burdensome. Additionally, adhering in good faith to a reasonable records management policy may assist in obtaining the protection of the safe harbor from sanctions under the Federal Rules of Civil Procedure, and some state rules, where ESI was lost as a result of the routine, good faith operation of an information system before a duty to preserve arose. Companies should be aware, however, that this safe harbor may not be available where the sole or primary purpose of a retention period in a records management policy is to make the information unavailable in litigation.

Maintain Current and Historical Organizational Charts. The importance of organizational charts was highlighted in the *Qualcomm* e-discovery debacle, where their absence was cited as a factor in the failure to identify thousands of key emails. Companies should consider maintaining accurate current and historical organizational charts that show their personnel at every level, and where they fit within the organization's structure. Companies that lack such organizational charts may face significant challenges in promptly identifying preservation and production custodians, and in effectively implementing a legal hold. Such companies may need to divert limited internal resources or pay for outside counsel to investigate and create such charts from scratch, which can be an expensive and time-consuming undertaking for a large organization.

Identify Subject Matter Experts. Identify and designate individuals who are knowledgeable about the company's information systems and processes and who can effectively coordinate with inside and outside counsel. This increases efficiency and accountability. Similarly, identify an appropriate individual who can serve as the "person most knowledgeable" about the company's records management, information systems and processes in the event there is a need to provide testimony about them.

Create a Data Map. A data map is a listing of the organization's ESI by category, location, and custodian or steward, including details on its storage, accessibility, associated retention policies, and procedures. Creating a data map may become increasingly important as the volume of ESI within an organization grows. The company should consider developing a position regarding which data sources are "not reasonably accessible," and therefore presumptively not discoverable (but still subject to a duty to preserve) or appropriate for cost-shifting. The company should apply this approach consistently to avoid undermining its defensibility. And it should be prepared to detail the specific burdens and costs that accompany the discovery of a particular data source for the benefit of the court.

Assess Whether Retention Periods May Pass the "Good Faith" Test. Some cases have found that the safe harbor for ESI lost as a result of the routine, good faith operation of an information system is unavailable where the company should have known that its records management practices would make relevant information unavailable to likely litigation opponents. Accordingly, companies may benefit from reviewing their records management practices, retention periods and "auto-delete" processes to assess whether a court might find that they have not satisfied the good faith requirement.

Develop a Legal Hold Policy and Procedures. In scuba diving, it is often said that divers should "plan the dive and dive the plan." The same is true with respect to legal holds. Companies will benefit from developing procedures for the implementation of legal holds. Doing so will ease the burden of meeting preservation obligations and help ensure that legal holds are implemented in a timely, consistent, appropriate and defensible manner. For example, companies should consider designating personnel to be responsible for identifying and analyzing potential triggers of the duty to preserve, and for implementing and overseeing a hold once the duty is triggered. Additional proactive steps include having legal hold notice templates ready that can be customized as needed, creating a process for administering the hold notice, tracking receipt and acknowledgement among hold notice recipients, and monitoring compliance with the legal hold.

Develop a Preservation Plan. Companies should consider developing an appropriate preservation plan in advance, with flexibility built in for exceptional circumstances. There are a number of different approaches to preserving ESI—including preserving in place, segregating files onto a designated legal hold server or disk drive, copying data so that redundant copies exist, and preserving on backup media. Each carries attendant costs, benefits and risks. For example, preserving in place may cost less, but also may in some circumstances increase the risk of spoliation. Relying on backup tapes to store active data for a legal hold may be convenient initially, but restoring it later may be time consuming, difficult and expensive on certain systems. Preserving onto a legal hold server or disk drive may be safe and effective, but it may also take up significant storage space on the company's systems.

Develop a Contingency Plan to Suspend Auto-Delete and Recycling of Backup Tapes. A plan for promptly suspending relevant auto-delete and purging functions, backup tape recycling, and default retention periods can assist in ensuring against spoliation once a duty to preserve attaches. Adequately labeling, storing, and indexing backup tapes can help ensure they are located in a timely fashion.

Take into Account Hardware and Software Upgrades. When companies roll out new laptops and workstations, the hard drives on those being replaced may be wiped, destroyed or sold to a new owner. Similarly, ESI may be lost or altered with software upgrades. Developing procedures to protect and retain the ESI of individuals subject to a legal hold can help ensure that relevant ESI is not destroyed in such circumstances.

Develop Exit Procedures for Departing Employees. Establish procedures to preserve and collect the ESI and hard copy documents of departing or transferring employees. Without advance planning, relevant ESI and hard copy documents may be lost or destroyed when an employee departs the company or transfers to a different office or department.

Plan for E-Discovery with Cloud and Other Third-Party Providers. Companies are increasingly using cloud providers and other third-party services for offsite storage of ESI. In these circumstances, companies should consider imposing retention, security and backup requirements on the third-party provider. Additionally, they should consider reaching an agreement in advance with the provider regarding the process for preserving and collecting ESI subject to a legal hold. If a company elects to use cloud-hosted email, then it is important to consider the ramifications for litigation. The willingness of a provider to take litigation preparedness into account may influence the company's decision regarding which provider to choose.

Evaluate and Select Preferred E-Discovery Vendors in Advance. Consider selecting a pool of preferred e-discovery vendors, including conducting due diligence and negotiating terms and pricing, in advance of litigation or an investigation. There is no need to be locked into just one vendor, as different vendors may be appropriate for different cases. Creating a pool of preferred e-discovery vendors in advance can save valuable time, as the process of hiring a vendor that the company has not previously vetted may take several days or even weeks. Doing so may also put the company in a better negotiating position regarding terms and pricing. Remember, however, that the least expensive vendor may not be the most appropriate for the needs of a significant case. Outside counsel may be able to recommend appropriate vendor candidates.

Audit the Company's Preparedness for E-Discovery. Similar to testing the security of a company's IT system by hiring outside consultants to attempt to breach it, consider testing the company's litigation preparedness via periodic auditing. A neutral third party can run a drill of a likely litigation scenario against the company's current practices and policies, thus exposing any deficiencies. Given that the ESI landscape is constantly changing, auditing also prevents established procedures from becoming stale and outdated.

In the next installment of E-Discovery Basics, we will discuss legal holds.

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

*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)