The Path from a "Good" to an "Excellent" Discovery Program

The Fundamental Value of Due Diligence

Submitted by
Jonathan M. Redgrave
James A. Sherer[1]
Redgrave LLP

Washington, D.C.
October 25, 2011

[1] Jonathan Redgrave is a Partner at Redgrave LLP and also Chair Emeritus of The Sedona Conference Working Group on Electronic Document Retention and Production. James Sherer is a Partner at Redgrave LLP. The views expressed in this article are those of the authors and not necessarily those of their firm. This article was originally prepared for R. Stanton Dodge for inclusion in materials for the December 7, 2011 Institute for Corporate Counsel program sponsored by the University of Southern California's School of Law.

> The "failure to conform to [the appropriate standard of care in discovery] is negligent even if it results from a pure heart and an empty head."
>
> *Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities, LLC*, 685 F. Supp. 2d 456, 464 (S.D.N.Y. 2010).

Those organizations that take their discovery programs from "good to excellent" seem to realize just what "due diligence" means in practice—both proactively and in any given case. In particular, we believe emerging case law and secondary authorities support the following twelve principles[2] that should be assessed and addressed by organizations when examining how to take a discovery program from good to excellent.

1. Be Prepared. Programs that have evolved from "good to great" understand the value of the Boy Scout Motto: "Be Prepared." Being prepared does *not* mean knowing where every single piece of paper or electronic document is stored, nor does it mean having a detailed process addressing every conceivable situation. It does mean having a fundamental awareness of significant data systems and business processes, as well as a comprehensive understanding of the company's litigation profile. It also means having response processes and systems in place which allow the company to preserve and collect documents and information when necessary.

2. Keep it Simple. Creating legal hold and collection processes throughout an organization does not require the development of a thousand page manual that must be read and followed by employees and counsel. The level of direction and documentation will necessarily vary among employees and the legal and IT staff responsible for taking certain actions. But in every circumstance, take excellent care to ensure that the instructions and training materials are as simple as possible. Use plain English and use examples. Taking the time to avoid ambiguity is taking the time to avoid trouble down the road.

3. It is a Process, not a Project. Due diligence in the context of a discovery response program is never-ending. It requires constant knowledge transfer by and between different constituencies, including Legal, IT, and the records management function, among others. An organization cannot simply hang a banner stating "Mission Accomplished"—the price of excellence is eternal vigilance.

4. Act Timely. Due diligence includes constant awareness of when a preservation duty has been triggered. An organization's representatives must act reasonably promptly upon such circumstances to preserve information, including distributing appropriate

[2] Certain sections of this paper, including a number of the twelve principles, are adapted from earlier works by Mr. Redgrave, including a paper for the 2010 ABA National Institute ABA-CLE, Section of Litigation, 4th Annual National Institute on E-Discovery (Washington, D.C., May 27, 2010) (with Amanda Vacarro), which in turn was based on materials submitted by Jonathan Redgrave and Dawson Horn III for the Georgetown E-Discovery Academy in February 2010 entitled "A Good Heart is Not Enough: The Need for Due Diligence." (Dawson Horn is in-house counsel at Tyco International in Princeton, New Jersey). The checklists at the end of the article are drawn from the original text of materials prepared by the Hon. Shira A. Scheindlin and Jonathan M. Redgrave, Discovery of Electronic Information in the revised edition of the treatise Business and Commercial Litigation in Federal Courts (West Publishing) (December 2005 through 2011).

legal hold notices. Keep in mind that this duty to preserve applies not only when claims may be brought against the organization, but also when the organization concludes that it may pursue legal action to enforce its own claims.

5. Follow Through. Excellence requires that legal hold notices and other preservation actions are not treated as self-executing. Monitoring may be required to ensure that directions are followed and relevant information is preserved. An appropriate follow-up may take different forms, but always incorporates an understanding of what has been done, and what, if anything, still needs to be done to discharge those legal obligations related to preservation and collection.

6. Perform a Factual Investigation. Due diligence does not end when a legal hold is issued. And while useful, having a legal hold software tool or a process book on the shelves is not enough. Excellent discovery response programs include processes that involve independent investigation into potential sources of relevant information, and take appropriate steps to ensure preservation and, as necessary, collection. Organizations with excellent programs recognize that tools, data maps, and flowcharts are not substitutes for actual custodian interviews and other means of investigation.

7. Cultivate Adaptability. Moving from good to excellent involves constant attention to existing circumstances to determine if additional action is needed. Have the facts and circumstances changed such that a new legal hold notice is needed? Are pertinent employees being terminated, such that additional preservation actions are needed? These and other questions must be asked, and asked consistently and continually, in order to exercise due diligence.

8. Document Your Story. An organization is well-served when it documents the decisions made and steps taken to preserve, collect, and produce relevant paper documents and electronically stored information. A contemporaneous record allows an organization to best defend its decisions and actions if ever challenged.

9. Enable Clear, Accurate, and Truthful Representations. It may seem elementary, but due diligence includes confirming that representations to opposing counsel, regulators, investigators, and courts are clear, accurate, and truthful. The case law is littered with examples of misleading, inaccurate and, at times, untruthful representations that ultimately form the heart of sanctionable conduct.

10. Know and Follow the Rules. Now more than ever, courts expect parties to take their Rule 26(f) meet and confer obligations seriously, and to pay scrupulous attention to what is required under Rule 34 for both narrowly tailored discovery requests and timely and meaningful responses (i.e., not boilerplate). Knowing the Rules also means knowing and understanding the availability of protections in the federal system against the inadvertent waiver of privilege, including those afforded by a properly drafted court order entered pursuant to Fed. R. Evid. 502(d).

11. Remember the People. Due diligence requires witnesses who have been an active part of the preservation and collection story—witnesses who know how to truthfully and accurately present that story. Discovery compliance, including preservation and collection, should be a component of all witness testimony preparation. Do the organization's witnesses know when they received a legal hold notice? Do they understand its contents and import? Do they recall what they did in response? They had better know (and be prepared for incisive questions), because of the significant chance they will be asked those questions in depositions or when taking the witness stand. An organization which helps its witnesses to prepare for these types of questions may avoid some of the surprises discovery can provide.

12. Involve People with Knowledge. To create and sustain an excellent discovery program, an organization must reach out and make use of people who have the requisite knowledge. This knowledge includes both factual (i.e., witnesses) and legal (i.e., counsel) development. Does the organization have the right internal resources? Are they well trained? Can outside counsel resources understand and execute the program? Who will be in charge when there are problems or charges of spoliation? Build a team wisely, with the intent of involving them over the long term.

Of course, taking your discovery program from "good to excellent" requires even greater depth than that addressed above. In addition to those broad principles, proper processes must also address the following expectations:

- Issuing written legal hold notices as soon as possible, following the "reasonable anticipation of litigation;"
- Continually reviewing the scope of the hold notice as additional potential custodians and responsive information are identified, and issuing updated holds as necessary;
- Implementing a system which tracks the litigation hold notice distribution and acknowledgments of receipt;
- Documenting the litigation hold process, so that an organization can respond to the question of "who received what notice when?";
- Preparing to meet and confer with opposing parties and the court regarding legal hold issues, including their distribution and related preservation efforts;
- Documenting those preservation measures that reflect a reasonable, good faith effort to preserve relevant information, especially if there are special circumstances where a written litigation hold notice is not feasible or appropriate;
- Providing instructions to custodians that are sufficient to effectively communicate what must be done to preserve potentially relevant information;
- Making good faith efforts to identify key players and others who may have potentially responsive information, to ensure that they receive hold notices and appropriate collection steps are undertaken;
- Using a process by which relevant information can be collected from key players, and others if necessary, at the outset of a matter;

- Using a process, where appropriate, by which forensic images of hard drives and other storage devices can be made and preserved if necessary; and
- Ensuring that the organization will be able to competently discuss, with opposing parties (and the court), the contours of what is and is not being done with respect to preservation and collection, and to identify and resolve any disputes early in the litigation.

Consistent with this best practices guidance, organizations should also consider the following initiatives to help their discovery program go from good to excellent:

- Developing and documenting a good working understanding of all backup systems, so that timely and defensible decisions can be made as to whether any backup media needs to be taken out of ordinary rotation and preserved;
- Establishing a process for timely identification and preservation of backup tapes which the organization believes contain unique and relevant information from key custodians in a given case;
- Preparing to discuss, with opposing parties (and the court), the organization's backup systems and which, if any, steps should be taken to preserve and/or produce such data;
- Preparing to defend, with a developed factual record, decisions made not to retain backup data; and
- Developing factual support for an argument that the restoration, processing, and production of content from retained backup media imposes an "undue burden or cost," such that the data is "not reasonably accessible" and thus should not be discovered (or, alternatively, if good cause would warrant such production, then there should be an allocation of the costs of such discovery).

These are starting points, not ending points. Each organization and circumstance is unique. But clearly, standing still or expecting that greatness "just happens" in this area is wrong. Excellence in the discovery process requires a significant investment in time and resources to establish the mindset, tools, and processes. But while the investment is significant, those organizations that make the investment subsequently report significant gains in both defensibility and efficiencies.

The additional checklists set forth below in Attachment A may be of assistance in helping your organization understand areas to address—both in proactive planning and in case responses. These checklists are excerpted from Shira A. Scheindlin and Jonathan M. Redgrave, *Discovery of Electronic Information* in the revised edition of the treatise *Business and Commercial Litigation in Federal Courts* (West Publishing) (December 2005 through 2011) (with Hon. Shira A. Scheindlin).[i] Please note, however, that none of these checklists present a "one size fits all" solution; instead, they present starting points for consideration and further analysis. Organizations must appropriately conform these lists to their size, organizational structure, and IT architecture, as well as its specific litigation profile. Finally, Section B provides a Form Case Management Order with general provisions addressing production issues.

A. Checklists

Checklist: Interviews of Various Organizational Employees

The following checklist is intended as a guide to assist counsel in identifying the existence and location of potentially relevant electronically stored information when conducting litigation-related due diligence inquiries. The list, by its very nature, is both over-inclusive and under-inclusive. In particular, the facts and circumstances of any given case will dictate the nature and extent of preservation and production obligations, and by extension the necessary level of due diligence. With that caveat, counsel should review these possible topics to determine which areas need to be explored in any particular case.

[ ] Initial steps:

- identify information likely to be relevant to the claims and defenses in the litigation;
- identify employees likely to have knowledge and information relevant to the subject matter of the litigation;
- identify information services personnel (which can be difficult because the organization of information services departments varies among companies, and, given the dynamic nature of both technologies and applications, tends to change frequently);
- identify hardware support group personnel;
- identify the group responsible for system maintenance, backup tapes, and tape archives; and
- identify applications group personnel (e.g., email system administrators and others creating and supporting applications for specific departments or groups within the organization)

[ ] Inquiries that may be appropriate for employees who may possess relevant information can include:

- Computer hardware used:
  - desktop and/or laptop computers
  - home computers used for business purposes
  - other hand-held devices (e.g., Palm Pilots, Blackberries)

- Applications used:
  - email
  - instant messaging
  - message attachments
  - internet email
  - shared email systems with service providers, etc.
  - voicemail
  - desktop/laptop applications
  - word processing
  - spreadsheets
  - presentation software (e.g., PowerPoint, Word, and Illustrator)
  - office management software (e.g., calendars, task lists, and notes)

- databases
- server/mainframe applications
- report applications (i.e., applications that generate sales reports, quality assurance reports, etc.)
- report preparation and form applications (e.g., work/project status reports)
- shareware
- Internet and Intranet usage
- web logs (a/k/a "blogs" or "weblogs")
- Wikis
- Internal collaboration tools (e.g., SharePoint)
- Social networking sites (e.g., Facebook, MySpace, LinkedIn)
- Other communications (e.g., Twitter)

• Computer file storage:
  - retention of email and use of email files/folders on desktop/laptop hard drives or servers
  - retention of draft and final documents (reports, memoranda, etc.) on desktop/laptop hard drives or servers, particularly documents not otherwise retained in hard copy form[ii]
  - retention of downloaded files received from employees or other sources
  - retention of office management files (e.g., calendars and task lists)
  - retention of files or documents by administrative assistants or secretaries[iii] and
  - use of removable media (e.g., CD-ROMs, DVDs, floppy disks or thumb drives)

[ ] Particular information services' department management may be the best sources for the following information:[iv]

- overviews of departmental organization
- policies and procedures regarding business retention of data and applications
- overviews of tape archives and policies and procedures for retaining archived data and applications
- retrieval of archived data and applications
- overviews of backup and disaster recovery policies and procedures
- retention procedures pursuant to litigation holds and preservation orders
- overviews of applications and databases and identification of any applications portfolios
- overviews of email systems and history of email systems[v]
- overviews of hardware, including its location (e.g., mainframes, servers, or personal computers)
- number and location of personal computers (including any provided for home use)
- other supported handheld devices that store data or files

[ ] Information services or information security personnel may be the best source for the following information:

- backup frequency
- retention of backup tapes before overwriting
- overviews of disaster recovery systems and identification of any map or portfolio of disaster recovery[vi]
- overviews of tape archives and identification of archived historical data and applications
- databases or indices to archived tapes
- retrievability and capacity to load and read archived historical data and applications
- retention periods for archived data and applications
- use of password and encryption technologies
- retention of archived data and applications for litigation purposes

[ ] Email systems administrators are likely the best source of the following information:

- overviews of email system structure (e.g., number of servers, number of post offices and mailboxes)
- overviews of system capabilities (e.g., attachments or folders)
- volume of traffic
- maintenance and retention of message logs
- retention period for unread messages
- frequency of overwriting deleted items
- shared systems with service providers, suppliers, or the corporate family
- policies regarding system use
- retention for litigation purposes

[ ] The following inquiries may be directed to applications administrators:[vii]

- descriptions of pertinent applications
- descriptions of report formats[viii]
- identification of databases and descriptions of data sources and data entry
- descriptions of how data is edited (e.g., does new data replace old data in a field, and is historical data retained)
- descriptions of how the applications are backed up
- information on whether historical data is archived
- descriptions of whether applications have been significantly modified during the relevant time period and, if so, were prior versions of the applications retained and can they be reinstalled and can data or reports be replicated or generated

Checklist: Investigating the Hardware Environment

An organization's computer hardware environment should be investigated to determine which devices are available to employees, and where the devices are located. The information services department is likely the best source of information. The investigation should include:

[ ] Availability of desktop and laptop computers
[ ] Use of networks with servers
[ ] Use of mainframe computers
[ ] Use of other, hand-held devices that store information
[ ] Use of home-based or employee-owned personal computers and laptops that have remote access to the organization's hardware and may store information or files
[ ] Use of CDs or other digital media to store historical records
[ ] Use of digital voicemail systems that store messages for extended periods
[ ] Possible retention of tape recordings, for example, of video teleconferences

This inquiry is designed to determine where and how pertinent records might be stored and located. For example, if certain categories of employees are entitled to have remote access to the organization's system, home-based personal computers may contain pertinent and discoverable records that either have never been imported to the organization's hardware or may not have been retained by the organization.[ix] In light of the 2006 amendments to Rule 26(b)(2)(B) that address disclosure and discovery of information that is "not reasonably accessible," it is also important to assess the burdens and costs that may be involved in retrieving and producing electronically stored information from hardware, especially older or retired (legacy) systems.

Checklist: Investigating Backup Systems and Archives

Inquiries should be made of the appropriate information services or data security personnel to determine:

- [ ] The frequency with which backup tapes of data and applications are made (i.e., daily, weekly, monthly or at longer intervals)
- [ ] Schedules for recycling and overwriting retained backup tapes[3]
- [ ] Locations of backup tapes (on-site or off-site)
- [ ] The existence of additional sets of data and application disaster recovery tapes
- [ ] The existence of archived historical data and related applications
- [ ] The types of data and applications archived
- [ ] Locations in which archived materials are kept (on-site or off-site)
- [ ] Any ability to load and run archived data and related applications

[3] Outside counsel should be aware that corporate management and in-house counsel often are not fully aware of the backup and archived materials maintained by information services personnel. In many instances, the culture of information services departments is to retain historical information whenever possible in order to meet the potential demands of their clients—the users of the system—and such departments may be far more concerned about being unable to retrieve information than they are about storing too much of it that long ago became useless.

Checklist: Investigating Applications

The rapid expansion and use of email has captured the attention of litigators and legal commentators because some users consider email to be (1) less formal than other forms of business communication and (2) as transitory as a phone conversation. Consequently, users exercise less discretion in creating it. But email is only one type of business application that the litigator must investigate. Other types of applications include, but are not limited to:

- [ ] Engineering and computer assisted design ("CAD") applications that may have replaced blueprints
- [ ] Product ingredient and formula databases and applications
- [ ] Manufacturing quality assurance applications, data collection, and data storage
- [ ] Financial records data generation, storage, and related applications
- [ ] Supplier bidding and purchasing applications
- [ ] Product distribution and sales databases and applications including payment and accounts receivable data
- [ ] Advertising, marketing, and product promotion databases and applications
- [ ] Customer and consumer information databases and consumer contact and complaint databases and applications
- [ ] Accident and incident report databases and applications
- [ ] Product testing and research report generation databases and applications
- [ ] External and governmental relations databases and applications, including lobbying expenditures and political contributions
- [ ] Indices of stored files, records, and other document collections such as research or business libraries
- [ ] Litigation-related databases and applications[x]
- [ ] Corporate Internet websites that might include representations about products or services, product warnings, consumer "hotlines" or links to other corporate data sets
- [ ] Databases and applications shared with service providers and suppliers
- [ ] Document management systems such as iManage, PC Docs, or DOCS Open[xi]
- [ ] "Shareware" (i.e., applications that allow contemporaneous editing of a document that can be fed back to the author or originator of the document)
- [ ] Desktop and laptop applications including word processing, spreadsheet programs, database software, presentation software, and office management software
- [ ] Corporate "intranets" which contain items such as on-line corporate directories, corporate news and announcements, corporate policies and procedures, and corporate published statements
- [ ] Digital voicemail systems
- [ ] Video teleconferencing systems with possible analog or digital storage
- [ ] Web logs (a/k/a "blogs" or "weblogs")
- [ ] Use of alternative communication means (e.g., Twitter, SMS, MMS)
- [ ] Collaboration tools and spaces (e.g., SharePoint)
- [ ] Social networking site (e.g., Facebook, MySpace, LinkedIn)
- [ ] Wikis

Even this checklist is incomplete, especially for organizations who are sophisticated computer users. But if an organization has made a substantial investment in hardware and has an information services department or outside service provider, the organization likely has developed and

implemented a computer application for virtually all regularly conducted business activities. In light of the 2006 amendments to Rule 26(b)(2)(B) that address disclosure and discovery of information that is "not reasonably accessible," it is also important to assess the burdens and costs that may be involved in retrieving and producing electronically stored information contained on data applications, especially older or retired (legacy) systems.

B. Form

Form Case Management Order Provisions Governing Production Issues[xii]

WHEREAS, the Parties mutually seek to reduce the time, expense, and other burdens of discovery of certain electronically stored information ("ESI") and privileged materials, as described further below, and to better define the scope of their obligations with respect to preserving such information and materials;

NOW THEREFORE, the Parties stipulate as follows:

1. **Preservation Not Required for Not Reasonably Accessible ESI.**
    a. The Parties agree that, except as provided in subparagraph b, the Parties need not preserve the following categories of ESI for this litigation:
        i. Data duplicated in any electronic backup system for the purpose of system recovery or information restoration, including but not limited to, system recovery backup tapes, continuity of operations systems, and data or system mirrors or shadows, if such data are routinely purged, overwritten, or otherwise made not reasonably accessible in accordance with an established routine system maintenance policy;
        ii. Voicemail messages;
        iii. Instant messages that are not ordinarily printed or maintained in a server dedicated to instant messaging;
        iv. Electronic mail or pin to pin messages sent to or from a Personal Digital Assistant (e.g., BlackBerry Handheld) provided that a copy of such mail is routinely saved elsewhere;
        v. Other electronic data stored on a Personal Digital Assistant, such as calendar or contract data or notes, provided that a copy of such information is routinely saved elsewhere;
        vi. Logs of calls made from cellular phones;
        vii. Deleted computer files, whether fragmented or whole;
        viii. Temporary or cache files, including internet history, web browser cache, and cookie files, wherever located;
        ix. Server, system, or network logs; and
        x. Electronic data temporarily stored by laboratory equipment or attached electronic equipment, provided that such data is not ordinarily preserved as part of a laboratory report.
    b. Notwithstanding subparagraph a, if on the date of this agreement any Party has a policy established by management that results in the routine preservation of any of the categories of ESI identified in subparagraph a, such Party shall continue to preserve information that was preserved in accordance with that policy, even if the Party subsequently changes its policy so that such information will no longer be routinely preserved in the future. However, the Parties shall have no obligation, in response to general discovery requests, to search for, produce, or create privilege logs for ESI covered by this subparagraph b.

2. **Obligations Related to "Draft" Documents and "Non-Identical" Documents.**
    a. For the purposes of preserving potentially discoverable material in this litigation, and for purposes of discovery in this litigation, the Parties agree that a "draft" document, regardless of whether it is in an electronic or hard copy form, shall mean, "a version of a document shared by the author with another person (by email, print, or otherwise)." In addition, a

"non-identical" document is one that shows at least one facial change such as the inclusion of highlights, underlining, marginalia, total pages, attachments, markings, revisions, or the inclusion of tracked changes.

b. The Parties agree that they need not preserve for discovery a document before and after every change made to it, so long as "draft" documents, as defined by this paragraph, are preserved. The Parties further agree that they shall preserve any presently existing "non-identical" documents that are relevant to the subject matter involved in this action. A document that is identical on its face to another document, but has small detectable differences in the metadata, shall be considered an identical copy.

3. **No Discovery of Material Not Required to Be Preserved.** The Parties agree not to seek discovery of items that need not be preserved pursuant to paragraphs 1-2, above. If any discovery request is susceptible of a construction which calls for the production of items that need not be preserved pursuant to paragraphs 1-2, such items need not be provided or identified on a privilege log pursuant to Fed. R. Civ. P. 26(b)(5).

4. **Preservation Does Not Affect Discoverability or Claims of Privilege.** The Parties agree that by preserving information for the purpose of this litigation, they are not conceding that such material is discoverable, nor are they waiving any claim of privilege. Except as provided in paragraph 3, above, nothing in this stipulation shall alter the obligations of the Parties to provide a privilege log for material withheld under a claim of privilege.

5. **Other Preservation Obligations Not Affected.** Nothing in this agreement shall affect any other obligations of the Parties to preserve documents or information for other purposes, such as pursuant to court order, administrative order, statute, or in response to other anticipated litigation.

6. **No Duty to Collect and Produce ESI in Response to General Discovery Requests.** The Parties agree that there is no obligation to search for and produce ESI in response to the Parties' general discovery requests, or to identify on a privilege log ESI that may be responsive to such requests. However, the Parties shall be obligated to search for and produce reasonably accessible ESI in response to reasonable requests for production that expressly seek ESI, and to identify on a privilege log any such ESI sought to be withheld on privilege grounds in response to such reasonable requests for production.

7. **Privileged Materials Located in the Offices of Counsel for the Parties.** The Parties agree that, in response to general discovery requests, the Parties need not search for and produce, nor create a privilege log for, any privileged material which is located in the offices of counsel for the parties.

8. **Effect of Inadvertent Production of Documents.**
   a. Consistent with Federal Rule of Evidence 502, the inadvertent production of documents in connection with the litigation before this Court shall not waive any privilege that would otherwise attach to the documents produced in this litigation. In addition, to the fullest extent authorized by Federal Rule of Evidence 502(d), any applicable work-product protection or attorney-client privilege is not waived as to anyone who is not a Party to this action by disclosure connected with this action. The following procedure shall apply to any such claim of inadvertent production.
   b. Upon learning of the inadvertent production, the producing Party shall promptly give all counsel of record notice of the inadvertent production. The notice shall identify the

document, the portions of the document that were inadvertently produced, and the first date the document was produced. If the Party that produced a document claims that only a portion of the document was inadvertently produced, the Party shall provide with the notice of inadvertent production a new copy of the document with the allegedly privileged portions redacted.

c. Upon receiving notice of inadvertent production, or upon determining that a document received is known to be privileged, the receiving Party must promptly return, sequester, or destroy the specified information and any copies it has, and shall destroy any notes that reproduce, copy, or otherwise disclose the substance of the privileged information. The receiving Party may not use or disclose the information until the claim is resolved. If the receiving Party disclosed the information before being notified, it must take reasonable steps to retrieve and prevent further use or distribution of such information until the claim is resolved.
d. A Party receiving documents produced by another Party is under a good faith obligation to promptly alert the producing Party if a document appears on its face or in light of facts known to the receiving Party to be privileged.
e. To the extent that any Party obtains any information, documents, or communications through inadvertent disclosure, such information, documents, and communications shall not be filed or presented for admission in this case.
f. In the event the receiving Party disputes the assertion of privilege, the Parties shall meet and confer and the requesting Party shall either: (a) return the material to the producing Party for proper designation; or (b) present the information to the Court under seal for a determination as to whether the material is protected from disclosure.

9. **Entire Agreement.** This stipulation contains the entire agreement of the Parties relating to the subject matter of this stipulation, and no statement, promise, or inducement made by any Party to this stipulation that is not set forth in this stipulation shall be valid or binding, nor shall it be used in construing the terms of this stipulation.

10. **Effective Upon Signing.** This stipulation is effective upon execution by the Parties, without regard to filing with the Court, and may be signed in counterparts.

11. **Sanctions.**
    a. No Party shall seek sanctions pursuant to the Federal Rules of Civil Procedure, the contempt powers of the Court, or any other authority against the other Party for the failure to preserve electronic information that is not required to be maintained pursuant to paragraph 1;
    b. Nothing in this agreement shall give rise to a claim for sanctions for failure to preserve information prior to the effective date of this agreement.

12. **Meet and Confer Requirement.** The Parties agree that before filing any motion with the Court regarding electronic discovery or evidence, the Parties will meet and confer in a good faith attempt to resolve such disputes.

---

[i] The endnotes that follow are drawn from the original text of the Hon. Shira A. Scheindlin and Jonathan M. Redgrave, Discovery of Electronic Information in the revised edition of the treatise Business and Commercial Litigation in Federal Courts (West Publishing) (December 2005 through 2011).

[ii] If document management systems are used, documents (files) created by system users are likely to reside on a server and possibly on the user's personal computer hard drive. In addition, the user may have dedicated server space where

files may be located. In discovery, an opposing party may argue that a computer file is a different document than a hard copy of the document because of additional information archived by the application associated with the stored file. Certain word processing applications, for example, automatically generate information (referred to as "metadata") regarding create dates, edit dates, and so on that do not appear on a printed version of the document (file). Accordingly, consideration must be given to the retention of the computer-stored file even if a hard copy version has been made. The same consideration must be given to existing email even if a print version of the email has been retained in hard copy form.

[iii] Interviewing secretaries and administrative assistants to higher ranked executives and managers is a good policy. More senior personnel are less likely to maintain their own calendars and task lists or create their own documents and are not likely to know the manner in which their secretary or administrative assistant maintains computer files.

[iv] Developing a working relationship with information services department management and fostering an understanding of litigation demands on the part of management is crucial. The diversion of resources to litigation support is a significant concern because information services is frequently viewed by corporate management as "overhead" and the department's priorities are skewed toward client (user) services and satisfaction. Outside litigation counsel are not clients.

[v] Email systems have developed very rapidly. Larger organizations may have (or have had) multiple systems over time and multiple systems that were (or are) concurrently in use. Generally, email systems that have been taken off-line and replaced will not be pertinent because email associated with the system are unlikely to exist; however, an inquiry should be made to determine if any backup tapes of the system were archived and might contain email and attachments to email.

[vi] A disaster recovery system map or portfolio might provide a valuable overview of applications and databases.

[vii] The initial step is to identify the databases and applications that may contain relevant information and then identify the current and, if available, former applications administrators. As previously noted, applications administrators may be assigned by department, and the administrators assigned to relevant departments also may need to be interviewed. With respect to databases, interviewers should be aware of so-called "relational databases"—i.e., multiple databases maintained on an organization-wide basis from which specific information is accessed and processed to prepare reports formatted for particular departments or business purposes. System users likely are aware of only the reports formatted for their business use or the limited number of data fields that they can search.

[viii] In many applications, the systems administrator and programming staff have the capability of designing a large variety of reports limited only by the fields of data in the underlying database(s). A potentially significant discovery issue is whether the discovering party is entitled only to reports as generated in the ordinary course of business or to the underlying data and the application to formulate their own reports.

[ix] Home-based and employee-owned computers may present difficult issues relating to what is (and is not) within the organization's possession, custody, or control. Those issues are outside the scope of this form.

[x] Organizations involved in substantial litigation may have developed litigation support systems and applications that, although they are used by outside counsel, reside on company computers. Systems of that type create difficult issues that should be discussed when considering the effect of preservation orders.

[xi] Document management systems may be of particular significance because (a) the system may archive documents not existing in other forms and (b) the file for a document may contain information about the creation, editing, and distribution of the document that is not apparent on the face of the document.

[xii] This form order is adopted almost verbatim from the stipulated order in *United States v. Louisiana Generating*, No. 9-100 (E.D. La. Mar. 5, 2010). Counsel should consider whether these or additional terms should be included or excluded in the context of any given matter.