Best Corporate Practices

For Electronic Discovery 2010

David K. Isom

Caution: The law and technology of electronic discovery are evolving so rapidly that best practices constantly change. Here is a recent summary of electronic discovery best practices for a typical large American company.

1. SCOPE AND PURPOSE OF BEST PRACTICES

1(a) Purpose

The purpose of these best practices is to assist the company in preparing for and conducting electronic discovery that:

1. is competent and cost-effective;

2. complies with developing law in light of developing technology;

3. minimizes the risk of sanctions and other liability relating to electronic discovery.

1(b) Scope

These best practices apply to federal civil litigation in the United States and all state court litigation with electronic discovery practices similar to federal practice. These best practices may also apply to some extent to other dispute processes, criminal actions and government audits and investigations in which electronic discovery is allowed or required.

1(c) Definition

“Electronic discovery” is the process of locating, assessing, preserving, requesting, inspecting, processing, culling, reviewing, protecting, disclosing and using in a dispute data that was created or transmitted and then stored in electronic form (“electronically stored information” or “ESI”), even if the data is later printed and produced or used on paper.

1(d) Tailoring Best Practices to Specific Case

Many courts have adopted significant local rules governing electronic discovery. The law and technology applicable to electronic discovery are developing rapidly. These best practices may and should be modified where indicated by complexity, developments in law and technology, cost constraints, and other unique circumstances.

2. ENGAGING TRIAL AND ELECTRONIC DISCOVERY COUNSEL

In engaging trial counsel and litigation counsel for an action, the company's legal representative should discuss these best practices with trial counsel and electronic discovery counsel and reach agreement with counsel as to the implementation of these best practices in the action.

3. INFORMATION TECHNOLOGY, DOCUMENT RETENTION AND USAGE POLICIES

3(a) Document Retention Policies, Schedules and Practices

The company should adopt a written document retention and destruction policy, schedule and practice that: (1) specify what ESI is to be retained and for how long; (2) specify what ESI is to be destroyed; (3) define a process for retention and destruction that is measurable and auditable and that is measured and audited, and that clearly defines responsibility for retention and destruction.

3(b) Usage and Intellectual Property Policies for Email and Other ESI

The company should adopt written usage policies for email and other ESI that define ownership of data and intellectual property and limit employees' expectations of privacy.

3(c) Use of Retention and Usage Policies in Litigation

Retention and usage policies should be drafted on the assumption that they will be discoverable in some litigation.

4. ELECTRONIC DISCOVERY TEAM

4(a) Core Litigation Team

The core litigation team for electronic discovery consists of the company's legal department representative with responsibility for the action, trial counsel and electronic discovery counsel. The core litigation team should reach a written agreement early in the litigation as to who has what responsibilities for electronic discovery in light of the risks and benefits of the case, including agreement as to who will make certifications under FRCP 26(g) and similar certifications under oath as to the process, adequacy and integrity of the electronic discovery processes of the company and counsel in the case.

4(b) Electronic Discovery Counsel

Electronic discovery counsel is responsible for implementing these best practices competently and cost-effectively. All electronic discovery duties should be expressly allocated and specified in writing throughout the litigation.

4(c) Support

The core litigation team should assemble and manage the electronic discovery support indicated by the needs of the case, including, for example, in-house or third party information technology and records management specialists and technical and forensics vendors, experts and consultants. All electronic discovery services provided by third parties must be provided pursuant to a written agreement that specifies financial responsibility, the scope and schedule of services, and the cost and basis of measuring the cost of such services.

5. LITIGATION HOLD

The core litigation team should manage the issuance of a prompt litigation hold notice to all custodians reasonably likely to have control of potentially relevant ESI that may otherwise be deleted in the ordinary course of business. The company should consider whether third parties that may host, store, archive or otherwise manage ESI for the company should also receive the litigation hold notice. Promptly after the preservation duty arises, the core litigation team should send written preservation notices to all employees and agents of the company reasonably likely to have custody, possession or control of potentially relevant ESI. The notice should:

1. specify with reasonable particularity the scope of the ESI to be preserved, including the date range, subject matter and sources of the ESI to be preserved;

2. specify the short-term actions that the recipient should take and should not take to preserve relevant ESI;

3. request a response to the notice by a date certain acknowledging receipt of the notice and the recipient's agreement to comply with the request; and

4. notify the recipient of follow-up contacts by the sender of the notice.

The litigation hold is typically the first step in the preservation process described at paragraph 9 below.

6. INITIAL IT ASSESSMENT

Promptly after issuing the litigation hold, the core litigation team should discuss the potential costs and risks associated with electronic discovery in the pending litigation, including (1) the cost of processing ESI into a searchable database and (2) attorney review for relevance, responsiveness,

privilege, work product protection, protection of private and proprietary information, and importance. This assessment should be used to make early decisions as to possible settlement strategies.

A prompt, initial assessment of the company's information systems containing potentially relevant ESI should be conducted. The assessment should show volume by source, document type, and date range and serve as the basis for an estimated budget for the electronic discovery process.

7. COST, BURDEN AND IMPORTANCE OF ESI

Electronic discovery duties are limited by the factors in FRCP 26(b)(2)(C) and case law, including technological feasibility, volume, importance, amount at stake in the action, cost and burden, business interference, privacy, confidentiality, other available sources, and whether the ESI is likely to be duplicative or cumulative. The core litigation team is responsible for controlling the cost of electronic discovery consistent with the duties, risks and benefits of the particular litigation by:

1. managing the electronic discovery process and actors cost-effectively;
2. understanding the legitimate limitations that may be placed upon electronic discovery;
3. negotiating efficiencies with opposing counsel, including the phasing of discovery so as to delay or avoid the least valuable discovery; and
4. transferring to the opposing party certain electronic discovery costs.

8. WRITTEN STRATEGIC PLAN

The core litigation team should agree upon a written strategic electronic discovery plan in advance of the Rule 26(f) conference that is consistent with these best practices, and amend the plan as needed throughout the litigation.

9. PRESERVATION AND ACQUISITION

9(a) Preservation Plan for the Company's ESI

The duty to preserve ESI and other relevant documents and things that are reasonably likely to be relevant to a legal dispute typically arises when the particular dispute becomes reasonably foreseeable. The preservation process may employ reasonable and statistically-justified sampling techniques and selection criteria. The litigation hold described above is typically the first step of the preservation process.

Before the Rule 26(f) conference, counsel should create a written preservation plan that specifically identifies the personnel that will carry out preservation, and the reasonable details of the plan that will be carried out. In support of the creation of a preservation plan, it may be necessary to identify and interview custodians of potentially relevant ESI and the IT personnel that manage the enterprise data.

The core litigation team should follow up by communicating with recipients of the litigation hold notices as soon as practicable after the litigation hold notice is sent to assure that proper preservation is completed.

9(b) Preservation Letter to Opponent and Third Parties

Promptly after the preservation duty arises (normally within one week), counsel should send a written notice to the opponent and to third parties to preserve relevant ESI. The level of detail of this notice should be appropriate to the circumstances, and may include a description of the scope of ESI to be preserved and the presumptive sources of the ESI, a summary of applicable preservation duties, instructions about the preservation of metadata and deleted data, and the possible need for immediate intervention in archiving, overwriting and other processes that may destroy relevant ESI.

9(c) Acquisition

Counsel should oversee the creation of a written data acquisition plan that describes how the data will be moved from its source location (in the ordinary course of business) to a target location where it can be reviewed. The acquisition plan should identify the personnel responsible, steps required for its completion, deadlines for completion of each step, and a budget for the acquisition.

10. DOCUMENT RETENTION, DESTRUCTION AND USAGE POLICIES, MANUALS AND PRACTICES

10(a) Discovery of Company Retention Policies and Practices

When litigation is reasonably foreseeable, the core litigation team should promptly review the company's document retention and destruction policies, schedules and practices, and email and computer usage policies, manuals and practices, in order to assure that routine destruction processes are terminated or modified as needed to preserve the ESI relevant to the litigation.

10(b) Discovery of Opponent's Policies and Practices

The core litigation team should consider whether to discover the opponent's document retention and destruction policies, schedules and practices, and email and computer usage policies, manuals and practices, in order to discover and to prevent destruction of relevant ESI.

11. SCOPE AND LIMITS OF PRESERVATION AND PRODUCTION

11(a) Written Scope

Promptly after litigation is contemplated or foreseen, the core litigation team should agree upon a written specification of the scope (by time, person, subject matter, source and other applicable criteria) of the ESI that must be preserved and is reasonably likely to be requested or produced. This specification of scope should be reviewed throughout the litigation to determine what if any changes are needed in light of amendments to the pleadings, discovery requests, motions or rulings, or newly discovered information or evidence.

11(b) Disclosure of Limits of Preservation or Discovery

In appropriate cases, limits upon the scope of the ESI to be preserved or produced (including the limits described in paragraphs 12 and 13 below) and limits upon the preservation efforts being undertaken should be revealed to opposing counsel so as to test and establish the legitimacy of the limitation and to mitigate potential consequences arising from the limitations upon the scope of preservation or production.

12. INADVERTENT LOSS OF RELEVANT ESI

Before or in connection with the Rule 26(f) conference, counsel should identify by source and type all potentially relevant ESI that has been lost as a result of the routine, good-faith operation of an information system over which the company had custody, possession or control. If any such data is requested in the action, counsel should identify this data as a defense to a motion for sanctions in compliance with FRCP 37(e) and its state equivalents.

13. INACCESSIBILITY

Before or in connection with the Rule 26(f) conference, the core litigation team should analyze the company's relevant information systems and identify to opposing counsel by source and type the potentially relevant information that is inaccessible because of undue burden or cost within the meaning of FRCP 26(b)(2)(B). This ESI should be identified as inaccessible in lieu of producing the data unless, in consultation with the company representative, it appears that there are reasons to produce the data that outweigh the burden and expense.

14. EARLY ATTORNEY AND COURT CONFERENCES

Promptly after commencement of an action, counsel should meet with company legal and IT representatives and should understand the relevant company technology and litigation issues in order to make and communicate in writing informed judgments and

recommendations relating to the issues required by FRCP 26(f) & 16(b) or their state equivalents.

Counsel should confer early in the action with opposing counsel to attempt to achieve efficiencies and reach agreement on electronic discovery.

15. PROCESSING, CULLING AND DEDUPLICATING

In consultation with any electronic discovery consultants and processors, the core litigation team should draft a written data processing, culling and production plan and method as soon as practicable in the litigation that is cost-effective in light of the duties and limitations created by FRCP 26(b)(2)(C) or its state equivalents.

Prior to engaging in a document / ESI review effort, the core litigation team should consider the costs and benefits of removing redundant (de-duping) or irrelevant (filtering) information from an acquired dataset prior to its review. In some cases it may be appropriate to perform de-duping and/or filtering as part of data acquisition. However, before a litigation hold can be lifted from data in its source location, counsel should ensure that the acquired dataset is not under-inclusive due to the filtering used.

The culling and review process should allow early cost-effective cursory attorney review of the potentially relevant data by Boolean, concept and contextual search methods so that counsel can evaluate potential volumes and costs before the bulk of the review costs are incurred.

16. HOSTING

Prior to the legal review of the preserved ESI, the core litigation team should consider the costs and benefits of hosting alternatives (i.e., platforms that make the data available to multiple locations).

Hosting can be done in a variety of formats (e.g., TIFF, PDF and native). For each matter, considering the needs of the matter and the data formats involved, the core litigation team should select the formats for hosting, review and production. The processing (i.e., conversion) required to host, review and produce documents (including the overhead of “load” files) should be considered when selecting vendors and platforms.

17. ATTORNEY REVIEW

For substantial document reviews, the core litigation team should create a written plan for creating manageable datasets for review and ensuring quality control over reviews for privilege and relevance.

18. INITIAL DISCLOSURES

The core litigation team should evaluate the company's relevant information systems early in the litigation, and at latest before the attorney discovery conference required by FRCP 16(b) or its state equivalents, so as to be able to negotiate and make proper initial disclosures of relevant ESI in compliance with FRCP 26(a)(1) or its state equivalents.

19. DEPOSITIONS

Early in the litigation, the core litigation team should identify and prepare a witness or witnesses to testify as a company representative in Rule 30(b)(6) depositions and trial regarding issues concerning the sources of electronically stored information and the execution of the electronic discovery process described by these best practices.

Counsel should consider conducting early Rule 30(b)(6) depositions of the opponent to discover and evaluate the existence and relative value of potentially relevant ESI and to evaluate the opponent's compliance with preservation and production duties.

20. SUBPOENAS DUCES TECUM

20(a) Responding to a Subpoena Duces Tecum for ESI

In responding to a subpoena for the production or inspection of ESI, the core litigation team should protect the company against undue expense and unnecessary production as provided by FRCP 45 and its state equivalents.

20(b) Serving Subpoenas Duces Tecum for ESI

In serving subpoenas, counsel should define the scope of the subpoena as narrowly as is consistent with the needs of the case.

21. TECHNOLOGY AND FORENSICS

The core litigation team should:

1. determine cost-effective methods and technologies for identifying, acquiring, culling, hosting, reviewing, producing and using electronic discovery in the action;

2. analyze applicable legal issues to make informed decisions about what sources must be searched for relevant ESI, and what must be done to identify, preserve and produce deleted data, residual or fragmented data, metadata, archived and backup data, offsite data, inactive data and third party data; and

3. determine what forensics processes are required under the circumstances of the case.

22. REQUESTS FOR PRODUCTION AND RESPONSES TO REQUESTS; FORMAT

22(a) Seeking Production of ESI

In requesting the production of ESI in an action, a lawyer should specify the requested format of production for each category of ESI, taking into account the cost, accessibility, utility and metadata associated with the various formats available.

22(b) Responding to Requests and Producing ESI

In responding to requests for ESI as to which no format is specified, the lawyer should produce ESI in a format in which the ESI is ordinarily maintained or in a reasonably useable form that minimizes overall expense. Only one format is required, and true duplicates may be eliminated if it is economic to do so.

In responding to requests for ESI as to which format is specified, a lawyer should consider whether to comply with the request or negotiate or move for production in a different format. If the technology needed to read produced data is not generally commercially available, the producing party may need to produce the means, such as proprietary software, to read the produced ESI.

23. INTERROGATORIES

23(a) Seeking IT Information by Interrogatories

The core litigation team should consider whether interrogatories may be a cost-effective means of discovering certain information regarding an opponent's relevant information technology and systems.

23(b) Responding to Interrogatories by Producing ESI

In responding to interrogatories, counsel should consider whether to identify relevant ESI pursuant to FRCP 33(d) in lieu of answering the interrogatory.

24. INSPECTION

24(a) Requesting Inspection of IT Media

In the event of a palpable risk of the loss of relevant ESI, counsel should consider requesting expedited production or inspection of an opponent's information media subject to protocols that protect the privacy, privilege and similar interests of the opponent.

24(b) Defending Requests for Inspection

Counsel should resist requests for inspection where appropriate, and should, if inspection is allowed, seek the protection of irrelevant, privileged, confidential, private and other protected ESI.

25. PRIVILEGE AND WORK PRODUCT PROTECTION

Before producing privileged or protected ESI pursuant to the protective provisions of FRCP 26(b)(5)(B) and its state equivalents, the core litigation team should consider the risks that such production may create, including the potential use of such privileged or protected ESI in other potential actions as to which the protections of FRCP 26(b)(5)(B) may not apply. For high volumes of privileged and protected ESI, a lawyer should consider computer-assisted processes to identify and log privileged and protected ESI. The core litigation team should consider whether the appointment of a master pursuant to FRCP 53 or the engagement by both parties of a third party to manage privilege issues is warranted and cost-effective.

26. PRIVACY, CONFIDENTIALITY AND PROPRIETARY INTEREST IN ESI

The core litigation team should advise the company as to how to manage electronic discovery so as to protect the privacy, confidentiality and proprietary rights connected with information that is or may be discovered in the litigation, including by the proper use of protective orders and civil rules such as FRCP 5.2 & 26(b)(2) and their state equivalents.

27. SPOLIATION SANCTIONS

27(a) Avoiding Liability for Spoliation

The core litigation team should protect the company and the firm from potential liability for spoliation under applicable statutes, regulations, rules, tort law and the inherent power of a court by:

1. understanding the application of the preservation duty in the particular case;

2. understanding, discussing and reaching written agreement upon the costs, risks and benefits of measures that should be taken to reduce risk and what risks are acceptable under the circumstances.

27(b) Evaluating and Establishing Opponent's Liability for Spoliation

The core litigation team should advise the company about cost-effective measures to assure that the opponent either preserves and produces relevant, non-privileged ESI or is made accountable for spoliation.

28. ELECTRONIC EVIDENCE

Throughout discovery, counsel should evaluate evidentiary issues, including foundation, to assure that important, relevant and useful ESI is admissible at trial and to challenge the use by an opponent of inadmissible ESI.