# AMENDMENTS TO CIVIL DISCOVERY STANDARDS

# AUGUST 2004

## IV. DOCUMENT PRODUCTION

**10. The Preservation of Documents. When a lawyer who has been retained to handle a matter learns that litigation is probable or has been commenced, the lawyer should inform the client of its duty to preserve potentially relevant documents in the client's custody or control and of the possible consequences of failing to do so. The duty to produce may be, but is not necessarily, coextensive with the duty to preserve. Because the Standards do not have the force of law, this Standard does not attempt to create, codify or circumscribe any preservation duty. Any such duty is created by governing state or federal law. This Standard is, instead, an admonition to counsel that it is counsel's responsibility to advise the client as to whatever duty exists, to avoid spoliation issues.**

2004 Comment

The addition of the phrase "in the client's custody or control" in the first sentence is not substantive. It is intended as a reminder to counsel that documents in the control, as well as the custody, of a client should also be the subject of counsel's advice with respect to document preservation. This includes, for example, documents in the control of senior executives of a corporation.

The second sentence is added to indicate that the duty to preserve data prior to litigation may be different from the duties imposed either by agreement or court order once litigation has commenced. The duty to preserve, whatever its scope, will vary significantly over time, becoming more pronounced as litigation becomes more likely and once litigation is, in fact, commenced. Litigants often will be required to produce that which they had no duty to preserve.

The third sentence is added to clarify that the Standards do not have the force of law and do not purport to create any duty. All duties are created by governing state or federal law.

## VIII. TECHNOLOGY

**29. Electronic Information.**

**a. ~~Duty to Preserve~~ Identifying ~~-~~Electronic Information. In identifying electronic data that parties may be called upon, in appropriate circumstances, to preserve or produce, counsel, parties and courts should consider:**

**~~A party's duty to take reasonable steps to preserve potentially relevant documents, described in Standard 10 above, also applies to information contained or stored in an electronic medium or format, including a computer word-processing document, storage medium, spreadsheet, database and electronic mail~~: The following types of data: A. Email (including attachments);**

**B. Word processing documents;**

**C. Spreadsheets;**

**D. Presentation documents;**

**E. Graphics;**

**G. Animations;**

**H. Images;**

**I. Audio, video and audiovisual recordings; and**

**J. Voicemail.**

**ii. The following platforms in the possession of the party or a third person under the control of the party (such as an employee or outside vendor under contract):**

**A. Databases;**

**B. Networks;**

**C. Computer systems, including legacy systems (hardware and software);**

**D. Servers;**

**E. Archives;**

**F. Back up or disaster recovery systems;**

G. Tapes, discs, drives, cartridges and other storage media;

H. Laptops;

I. Personal computers;

J. Internet data;

K. Personal digital assistants;

L. Handheld wireless devices;

M. Mobile telephones;

N. Paging devices; and

O. Audio systems, including voicemail.

iii. Whether potentially producible electronic data may include data that have been deleted but can be restored.

~~ii. Unless otherwise stated in a request, a request for "documents" should be construed as also asking for information contained or stored in an electronic medium or format.~~

~~iii. Unless the requesting party can demonstrate a substantial need for it, a party does not ordinarily have a duty to take steps to try to restore electronic information that has been deleted or discarded in the regular course of business but may not have been completely erased from computer memory.~~

b. **Discovery of Electronic Information.**

i. Document requests should clearly state whether electronic data is sought. In the absence of such clarity, a request for "documents" should ordinarily be construed as also asking for information contained or stored in an electronic medium or format.

ii. A party ~~may ask~~should specify whether ~~for the production of~~ electronic information should be produced in hard copy~~, in electronic form or in both forms. A party may also ask for the production of~~, in electronic form or, in an appropriate case, in both forms. A party requesting information in electronic form should also consider:

A. Specifying the format in which it prefers to receive the data, such as:

I. Its native (original) format, or

II. A searchable format.

B. Asking for the production of metadata associated with the responsive data — *i.e.,* ancillary electronic information that relates to ~~relevant~~responsive electronic ~~documents~~data, such as information that would indicate ~~*(a)*~~ whether and when the responsive electronic ~~mail was sent or opened by its recipient(s) or *(b)* whether and when information~~data was created ~~and/or~~, edited, sent, received and/or opened. ~~A party also may request~~

C. Requesting the software necessary to retrieve, read or interpret electronic information.

D. Inquiring as to how the data are organized and where they are stored.

A party who produces information in electronic form ordinarily need not also produce hard copy to the extent that the information in both forms is identical or the differences between the two are not material.

~~ii.~~ iii. In resolving a motion seeking to compel or protect against the production of electronic information or related software, or to allocate the costs of such discovery, the court should consider such factors as:

A. The burden and expense of the discovery, considering among other factors the total cost of production in absolute terms and as compared to the amount in controversy;

B. The need for the discovery, including the benefit to the requesting party and the availability of the information from other sources;

C. The complexity of the case and the importance of the issues;

D. The need to protect the attorney-client privilege or attorney work product ~~privilege~~, including the burden and expense of a privilege review by the producing party and the risk of inadvertent disclosure of privileged

or protected information despite reasonable diligence on the part of the producing party;

E. The need to protect trade secrets, and proprietary or confidential information;

F. Whether the information or the software needed to access it is proprietary or constitutes confidential business information;

G. The breadth of the discovery request;

H. Whether efforts have been made to confine initial production to tranches or subsets of potentially responsive data;

I. The extent to which production would disrupt the normal operations and processing routines of the responding party;

J. Whether the requesting party has offered to pay some or all of the discovery expenses;

K The relative ability of each party to control costs and its incentive to do so;

L. The resources of each party as compared to the total cost of production; ~~and *(g)* the resources of each party.~~

M. Whether responding to the request would impose the burden or expense of acquiring or creating software to retrieve potentially responsive electronic data or otherwise require the responding party to render inaccessible electronic information accessible, where the responding party would not do so in the ordinary course of its day-to-day use of the information;

N. Whether responding to the request would impose the burden or expense of converting electronic information into hard copies, or converting hard copies into electronic format;

O. Whether the responding party stores electronic information in a manner that is designed to make discovery impracticable or needlessly costly or burdensome in pending or future litigation, and not justified by any legitimate personal, business, or other non-litigation related reason; and

P. Whether the responding party has deleted, discarded or erased electronic information after litigation was commenced or after the responding party was aware that litigation was probable and, if so, the responding party's state of mind in doing so.

**In complex cases and/or ~~ones~~ cases involving large volumes of electronic information, the court may want to consider using an expert to aid or advise the court on technology issues**

~~iii. The discovering party generally should bear any special expenses incurred by the responding party in producing requested electronic information. The responding party should generally not have to incur undue burden or expense in producing electronic information, including the cost of acquiring or creating software needed to retrieve responsive electronic information for production to the other side~~**.**

~~iv. Where the parties are unable to agree on who bears the costs of producing electronic information, the court's resolution should consider, among other factors:~~

~~*(a)* whether the cost of producing it is disproportional to the anticipated benefit of requiring its production;~~

~~*(b)* the relative expense and burden on each side of producing it;~~

~~*(c)* the relative benefit to the parties of producing it; and~~

~~*(d)* whether the responding party has any special or customized system for storing or retrieving the information.~~

~~v~~**iv.** **The parties are encouraged to stipulate as to the authenticity and identifying characteristics (date, author, etc.) of electronic information that is not self-authenticating on its face.**

2004 Comment

Subdivision(a)

Subdivision (a)(i). Standard 29(a)(i) is principally designed to provide a checklist to assist counsel in identifying types of electronic data as to which the duty to preserve may apply, once that duty has been triggered under applicable law. See, e.g., Super Film of Am., Inc. v. UCB Films, Inc., 219 F.R.D. 649, 657 (D. Kan. 2004) (for

purposes of Federal Rule of Civil Procedure 26, "[c]omputerized data and other electronically-recorded information includes, but is not limited to: voice mail messages and files, back-up voice mail files, e-mail messages and files, backup e-mail files, deleted e-mails, data files, program files, backup and archival tapes, temporary files, system history files, web site information stored in textual, graphical or audio format, web site log files, cache files, cookies, and other electronically-recorded information") (citation and quotations omitted).

This Standard is not intended to suggest that electronic discovery is appropriate in all cases. There may be many cases in which electronic discovery is not warranted, in light of the amount in controversy or any number of other reasons.

The deletion of the former first sentence of subdivision (a)(i) is intended to clarify that the Standards do not create or codify law but rather defer to governing substantive law. The purpose of the list provided in subdivision (a)(i) is to assist counsel in protecting client interests under whatever strictures may be imposed by governing law. It is not to suggest that every item in the list is applicable in every case or that counsel has any duty to instruct a client to preserve any, much less every, item on the list. All duties are dictated by governing state or federal law and not by this or any other of these Standards.

Subdivision (a)(ii). Just as subdivision (a)(i) provides a checklist of the types of electronic data that counsel should bear in mind, Standard 29(a)(ii) provides a checklist of platforms and places where such data may be found. As with subdivision (a)(i), subdivision (a)(ii) does not create a preservation duty. Rather, it is another reference tool intended to be consulted once the duty to preserve electronic data has accrued under local law.

Subdivision (a)(iii). Standard 29(a)(iii) is simply a reminder that, as is well established in the case law, when a preservation duty has been triggered, it may be found to apply to "deleted" information remaining on the hard drive of the computer. Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 313 n.19 (S.D.N.Y. 2003) ("The term 'deleted' is sticky in the context of electronic data. 'Deleting' a file does not actually erase that data from the computer's storage devices. Rather, it simply finds the data's entry in the disk directory and changes it to a 'not used' status -- thus permitting the computer to write over the 'deleted' data. Until the computer writes over the 'deleted' data, however, it may be recovered by searching the disk itself rather than the disk's directory. Accordingly, many files are recoverable long after they have been deleted -- even if neither the computer user nor the computer itself is aware of their existence. Such data is referred to as 'residual data.'")(internal quotations and citation omitted).

Former Subdivision (a)(ii). Former subdivision (a)(ii) has been moved to subdivision (b), where it conceptually belongs, as new subdivision (b)(i), with minor modification.

Former Subdivision (a)(iii). Former subdivision (a)(iii) has been deleted. As drafted, it appeared to create or codify a proposition of law, which is not the proper function of a Standard. Moreover, the law is evolving swiftly in the area of electronic discovery and, as stated, the deleted language is not necessarily good law. See, e.g., Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 324 (S.D.N.Y. 2003) ("because the cost-shifting analysis is so fact-intensive, it is necessary to determine what data may be found on the inaccessible media. Requiring the responding party to restore and produce

responsive documents from a small sample of the requested backup tapes is a sensible approach in most cases").

Subdivision(b)

Subdivision (b)(i). The second sentence of subdivision (b)(i) is the former subdivision (a)(ii), with the addition of a connecting dependent clause and the insertion of the modifier "ordinarily," the latter in recognition of the fact that there may be unusual circumstances in which the state presumption is obviously inapt. The new first sentence is added as a "best practices" reminder to counsel.

Subdivision (b)(ii). Subdivision (b)(ii) restates and expands the former subdivision (b)(i). The substantive additions are to remind counsel, first, that they have the option of specifying the format in which they wish to receive the desired data and, second, that they may want to inquire as to how the data were organized and where they were stored, since this information may be lost in electronic production.

Subdivision (b)(iii). Subdivision (b)(iii) combines the former subdivisions (b)(ii) and (b)(iv) in recognition of the fact that the factors applied by the courts in resolving motions to compel (or resist production) and motions to allocate costs are largely the same. Additionally, subdivision (b)(iii) expands the former subdivisions (b)(ii) and (b)(iv) to capture additional factors that experience and the developing case law have identified as pertinent to the court's decision. Among the authorities relied on in the recitation of factors in this subdivision are: Federal Judicial Center, Manual for Complex Litigation § 11.446 (4th ed. 2004); 7 Moore's Federal Practice §§ 37a.30-33 (3d ed. 2004); Zubulake v. UBS Warburg LLC, 217 F.R.D. 309 (S.D.N.Y. 2003); Zubulake v. UBS Warburg LLC, 216 F.R.D. 280 (S.D.N.Y. 2003); Computer Associates International, Inc. v. Quest Software, Inc., No. 02-C-4721, 2003 WL 21277129 (N.D. Ill. June 3, 2003); Medtronic Sofamor Danek, Inc. v. Michelson, No. 01-2373-M1V, 2003 WL 21468573 (W.D. Tenn. May 13, 2003); Dodge, Warren, & Peters Ins. Servs. v. Riley, 130 Cal. Rptr. 2d 385 (Cal. App. 2003); Byers v. Illinois State Police, 2002 WL 1264004 (N.D. Ill. June 3, 2002); Southern Diagnostic Assocs. v. Bencosme, 833 So.2d 801 (Fla. App. 2002); Murphy Oil USA, Inc. v. Fluor Daniel, Inc., 2002 WL 246439 (E.D. La. Feb. 19, 2002); Rowe Entertainment, Inc. v. William Morris Agency, 205 F.R.D. 421 (S.D.N.Y. Jan 16, 2002); In re CI Host, Inc., 92 S.W. 3d 514 (Tex. 2002); In re Bristol-Meyers Squibb Secs. Litig., 205 F.R.D. 437 (D.N.J. 2002); McPeek v. Ashcroft, 202 F.R.D. 31 (D.D.C. Aug. 1, 2001); McCurdy Group, LLC v. American Biomedical Group, Inc., Nos. 00-6183, 00-6332, 2001 WL 536974 (10th Cir. May 21, 2001).

Subdivision (b)(iv). Subdivision (b)(iv) is the former subdivision (b)(v) unchanged.

Former Subdivision (b)(ii). Former subdivision (b)(ii), together with former subdivision (b)(iv), is contained within new subdivision (b)(iii).

Former Subdivision (b)(iii). Former subdivision (b)(iii) has been deleted. As drafted, it appeared to create or codify a proposition of law, which is not the proper function of a Standard. Moreover, the law is evolving swiftly in the area of electronic discovery and, as stated, the deleted language is not necessarily good law. See, e.g., Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 324 (S.D.N.Y. 2003).

Former Subdivision (b)(iv). Former subdivision (b)(iv), together with former subdivision (b)(ii), is contained within new subdivision (b)(iii).

**30. Using Technology to Facilitate Discovery.**

**a. In appropriate cases, the parties may agree or the court may direct that some or all discovery materials that have not been stored in electronic form should nonetheless be produced, at least in the first instance, in an electronic format and how the expenses of doing so will be allocated among the parties.**

**b. ~~Upon request, a~~A party serving written discovery requests or responses should provide the other party or parties with ~~a diskette or other~~an electronic version of the requests or responses unless the parties have previously agreed that no electronic version is required.**

2004 Comment

Subdivision (a). This change is not substantive but merely clarifying. If the data sought in discovery already exist in electronic form, there is no need for a court order requiring their production in that format. This subdivision is directed at the production in electronic format of data not currently stored electronically. The amendment makes that clear.

Subdivision (b). Subdivision (b) has been amended to interpose a presumption where previously a request was suggested. As amended, this subdivision affirmatively recommends that counsel provide adversaries with discovery requests or responses in electronic format unless the parties have previously agreed to the contrary. Because the Standard is purely precatory, it imposes no duty. Rather, it recommends a practice for counsel to consider.

31. Discovery Conferences.

a. At the initial discovery conference, the parties should confer about any electronic discovery that they anticipate requesting from one another, including:

i. The subject matter of such discovery.

ii. The time period with respect to which such discovery may be sought.

iii. Identification or description of the party-affiliated persons, entities or groups from whom such discovery may be sought.

iv. Identification or description of those persons currently or formerly affiliated with the prospective responding party who are knowledgeable of the information systems, technology and software necessary to access potentially responsive data.

v. The potentially responsive data that exist, including the platforms on which, and places where, such data may be found as set forth in Standard 29 (a).

vi. The accessibility of the potentially responsive data, including discussion of software, hardware or other specialized equipment that may be necessary to obtain access.

vii. Whether potentially responsive data exist in searchable form.

viii. Whether potentially responsive electronic data will be requested and produced:

A. In electronic form or in hard copy, and

B. If in electronic form, the format in which the data exist or will be produced

ix. Data retention policies applicable to potentially responsive data.

x. Preservation of potentially responsive data, specifically addressing (A) preservation of data generated subsequent to the filing of the claim, (B) data otherwise customarily subject to destruction in ordinary course, and (C) metadata reflecting the creation, editing, transmittal, receipt or opening of responsive data.

xi. The use of key terms or other selection criteria to search potentially responsive data for discoverable information.

xii. The identity of unaffiliated information technology consultants whom the litigants agree are capable of independently extracting, searching or otherwise exploiting potentially responsive data.

xiii. Stipulating to the entry of a court order providing that production to other parties, or review by a mutually-agreed independent information technology consultant, of attorney-client privileged or attorney work-product protected electronic data will not effect a waiver of privilege or work product protection.

xiv. The appropriateness of an inspection of computer systems, software, or data to facilitate or focus the discovery of electronic data.

xv. The allocation of costs.

b. At any discovery conference that concerns particular requests for electronic discovery, in addition to conferring about the topics set forth in subsection (a), the parties should consider, where appropriate, stipulating to the entry of a court order providing for:

i. The initial production of tranches or subsets of potentially responsive data to allow the parties to evaluate the likely benefit of production of additional data, without prejudice to the requesting party's right to insist later on more complete production.

ii. The use of specified key terms or other selection criteria to search some or all of the potentially responsive data for discoverable information, in lieu of production.

iii. The appointment of a mutually-agreed, independent information technology consultant pursuant to Standard 32(a) to:

A. Extract defined categories of potentially responsive data from specified sources, or

B. Search or otherwise exploit potentially responsive data in accordance with specific, mutually-agreed parameters.

2004 Comment

The Federal Rules of Civil Procedure require a discovery conference at the outset of every case and prior to the filing of any discovery motion. Practices vary district by district. State court practice varies state by state, but a conference early in the case is sensible in connection with electronic discovery, regardless of whether it is compelled. Standard 31 focuses on effective use of discovery conferences to address electronic discovery issues.

Subdivision (a). Subdivision (a) focuses on the initial discovery conference. It specifies several categories of electronic discovery related matters that the parties should confer about at an initial discovery conference. It is intended to assist counsel and the court by providing a detailed array of potentially relevant issues to address. These include:

- Subject matter
- Relevant time period
- Identification of the party-affiliated persons or entities from whom electronic discovery may be sought
- Identification of those persons (including former employees) who are knowledgeable of the information systems, technology and software necessary to access potentially responsive data
- The universe of potentially responsive data that exist, including the platforms on which, and places where, such data may be found (including databases, networks, systems, servers, archives, back up or disaster recovery systems, tapes, discs, drives, cartridges and other storage media, laptops, PCs, Internet data, and PDAs)
- Accessibility issues, such as the software that may be necessary to access data
- Whether potentially responsive data exist in searchable form
- Whether potentially responsive electronic data will be requested and produced in electronic form or in hard copy
- Data retention policies
- Preservation issues, including preservation of data generated subsequent to the filing of the claim
- Possible use of key terms or other selection criteria to scour massive amounts of data for relevant information

Anticipating the privilege-related issues addressed in Standard 32, subdivision (a)(xii) suggests that the parties discuss whether they can agree on the names of unaffiliated information-technology consultants who would be capable of serving them jointly, either in a privately-retained or court-appointed capacity. In the same vein, subdivision (a)(xiii) proposes that the parties consider whether it would be desirable for them to stipulate to entry of a court order along the lines discussed in Standard 32(b) or (c).

Subdivision (b). Subdivision (b) focuses on discovery conferences relating to outstanding discovery requests (in common parlance, the "meet-and-confer"). It recognizes that there are additional issues for the parties to consider once discovery demands have been served and specific issues are on the table. Subdivision (b) anticipates a number of the privilege-related initiatives contained in Standard 32, recommending that the parties consider stipulating to a court order providing for:

- Initial production, on a without-prejudice basis, of subsets of electronic data to allow the parties to evaluate the likely benefit of production of additional data;

- The use of search terms or other selection criteria in lieu of production; or

- The appointment of an independent consultant pursuant to Standard 32

32. Attorney-Client Privilege and Attorney Work Product. To ameliorate attorney-client privilege and work product concerns attendant to the production of electronic data, the parties should consider, where appropriate, stipulating to the entry of a court order:

a. Appointing a mutually-agreed, independent information technology consultant as a special master, referee, or other officer or agent of the court such that extraction and review of privileged or otherwise protected electronic data will not effect a waiver of privilege or other legal protection attaching to the data.

b. Providing that production to other parties of attorney-client privileged or attorney work-product protected electronic data will not effect a waiver of privilege or work product protection attaching to the data. In stipulating to the entry of such an order, the parties should consider the potential impact that production of privileged or protected data may have on the producing party's ability to maintain privilege or work-product protection vis-à-vis third parties not subject to the order.

c. Providing that extraction and review by a mutually-agreed independent information technology consultant of attorney-client privileged or attorney work-product protected electronic data will not effect a waiver of privilege or work product protection attaching to the data.

d. Setting forth a procedure for the review of the potentially responsive data extracted under subdivision (a), (b), or (c). The order should specify that adherence to the procedure precludes any waiver of privilege or work product protection attaching to the data. The order may contemplate, at the producing party's option:

i. Initial review by the producing party for attorney-client privilege or attorney work product protection, with production of the unprivileged and unprotected data to follow, accompanied with a privilege log, or

ii. Initial review by the requesting party, followed by:

A. Production to the producing party of all data deemed relevant by the requesting party, followed by

B. A review by the producing party for attorney-client privilege or attorney work product protection. Before agreeing to this procedure, the producing party should consider the potential impact that it may have on the producing party's ability to maintain privilege or work-

**product protection attaching to any such data if subsequently demanded by non-parties.**

**The court's order should contemplate resort to the court for resolution of disputes concerning the privileged or protected nature of particular electronic data.**

**e. Prior to receiving any data, any mutually-agreed independent information technology consultant should be required to provide the court and the parties with an affidavit confirming that the consultant will keep no copy of any data provided to it and will not disclose any data provided other than pursuant to the court's order or parties' agreement. At the conclusion of its engagement, the consultant should be required confirm under oath that it has acted, and will continue to act, in accordance with its initial affidavit.**

**f. If the initial review is conducted by the requesting party in accordance with subsection (d)(ii), the requesting party should provide the court and the producing party an affidavit stating that the requesting party will keep no copy of data deemed by the producing party to be privileged or work product, subject to final resolution of any dispute by the court, and will not use or reveal the substance of any such data unless permitted to do so by the court.**

2004 Comment

Standard 32 deals with privilege and work product (collectively, "privilege") concerns. It applies in the common situation in which electronic data must be extracted for production by an information technology (IT) expert not employed by the producing party. This scenario by definition raises a risk of waiver because privileged documents are being exposed to persons outside the privilege. Standard 32 sets forth three methods to ameliorate the risk of waiver. Each would be implemented by entry of a stipulated court order.

Subdivision (a). Subdivision (a) suggests that the parties consider having the court appoint a mutually-agreed IT consultant as a special master, referee, or other officer of the court, so that the consultant's extraction and review of privileged electronic data will not effect a waiver. This approach would allow the third party consultant to pull and have access to privileged material (which may be included in any mass extraction of data) without risk that the holder of the privilege will have effected a waiver by permitting the third party to review them. Following extraction, the parties are then free to specify whatever protocol they prefer with respect to review of the data. This is addressed in subdivision (d).

Subdivision (b). Subdivision (b) addresses what is sometimes known as the "quick peek" approach to electronic discovery. Under the quick-peek scenario

envisioned by subdivisions (b) and (d)(ii), the requesting party may have sufficient resources to perform or pay for the extraction, and the producing party may be inclined to allow its opponent to incur all expenses associated with doing so. At the same time, the producing party has no interest in waiving privilege. The parties therefore agree that the data will be turned over to the requesting party without review by the producing party; the requesting party will identify which documents it is interested in, and the producing party will then conduct a privilege review. Subdivision (b) captures the court order necessary to permit this procedure to proceed.

Under subdivision (b), the parties stipulate to an order providing that production of privileged electronic data will not effect a waiver. Note that this is different from the customary agreed order, which provides that inadvertent production will not effect a waiver, because parties using the subdivision (b) approach may know or be fairly certain that privileged material is contained in the mass of data to be extracted. Like that order, however, there is some question as to the effectiveness of such an order vis-à-vis a third party who subsequently seeks the disclosed data. Accordingly, there is an appropriate caution in the text of this subdivision and in subdivision (d)(ii).

Subdivision (c). Subdivision (c) is similar to subdivision (a) in that it envisions the use of an agreed third-party consultant. Under subdivision (c), unlike subdivision (a), that consultant is not appointed as a special master or other court officer. The court, for example, may not be inclined to appoint the consultant as a master or the parties may prefer to control the consultant directly. Subdivision (c) is also similar to subdivision (b) in that it envisions the entry of an order providing that review of intentionally-produced privileged data will not effect a waiver. But the reviewing party under subdivision (c) is an agreed-on consultant, not the opposition. As under both subdivisions (a) and (b), under subdivision (c) the parties are free to specify whatever protocol they prefer with respect to review of the data, following extraction. This is addressed in subdivision (d).

As observed in the comment to subdivision (b), supra, in current practice, there is no assurance that a stipulated order providing that inadvertent production does not effect a waiver will be effective against a claim of waiver asserted by a third party. Precisely the same risk is posed by the order envisaged by subdivision (c). Accordingly, it is imperative that litigants following either of these routes also have in place a confidentiality order as a second line of defense against inquisitive third parties. It is equally important that the litigants develop a protocol for, or otherwise instruct, the consultant to minimize the likelihood that the consultant will actually review (as opposed to extract) privileged material.

Subdivision (d). Subdivision (d) sets forth a pair of alternative procedures for the parties to consider with respect to the review of the data once the data have been extracted. Subdivision (d)(i) states that traditional approach, in which the extracted data are furnished to the producing party, who then conducts a review for responsiveness and privilege, and makes production of the data together with a privilege log.

Subdivision (d)(ii) identifies an unconventional approach that some parties prefer for financial reasons, as where there is an enormous amount of electronic data, little of it is likely to be either responsive or privileged, and little of that will fall in both categories. Under the (d)(ii) approach, the requesting party first reviews the data for responsiveness and provides to the producing party all data in which it is interested. The producing party then determines if any of the data in question are privileged. If so, the requesting party may not maintain copies of the privileged material unless and until a court sustains its objections to the claim of privilege. This procedure raises the risk of waiver of privilege identified in the comment to subdivision (b). Accordingly, the text of subdivision (d)(ii)(B) contains substantially the same caution as that set forth in subdivision (b).

Subdivision (e). Subdivision (e) suggests a reasonable precaution — that any IT consultant employed by the parties be required to execute an affidavit confirming that it will keep no copy of any data and will not disclose any data provided other than pursuant to the court's order or parties' agreement.

Subdivision (f). Subdivision (f) provides that, before receiving the data pursuant to subdivision (d)(ii), the requesting party is to execute an affidavit stating that it will keep no copy of data deemed by the producing party to be privileged, subject to final resolution of any dispute by the court. This precaution is appropriate in light of the trust that the producing party reposes in the requesting party under the quick-peek approach captured in subdivisions (b) and (d)(ii).

**33. Technological Advances. To the extent that information may be contained or stored in a data compilation in a form other than electronic or paper, it is intended that Standards 29-32 may be consulted with respect to discovery of such information, with appropriate modifications for the difference in storage medium.**

2004 Comment

Standard 33 recognizes the impracticability of keeping pace with technological change. New, non-electronic media may emerge for the creation or retention of electronic data. This Standard suggests that Standards 29-32 be consulted with respect to discovery of such data, subject to common sense modifications.