Section Chair
David H. Tennant

Immediate Past Section Chair
Jonathan D. Lupkin

Co-Chair of the
E-Discovery Committee
Constance M. Boland

Co-Chair of the
E-Discovery Committee
Adam I. Cohen

NYSBA

Best Practices In E-Discovery In New York State and Federal Courts

Report of the E-Discovery Committee of the Commercial and Federal Litigation Section of the New York State Bar Association

July 2011

Approved by the NYSBA Executive Committee, September 27, 2011

TABLE OF CONTENTS

Page

Members of the E-Discovery Committee ..... (i)

Introduction 1

Guideline No. 1 3

Guideline No. 2 5

Guideline No. 3 6

Guideline No. 4 9

Guideline No. 5 10

Guideline No. 6 12

Guideline No. 7 14

Guideline No. 8 16

Guideline No. 9 18

Guideline No. 10 20

Guideline No. 11 23

Guideline No. 12 25

Guideline No. 13 27

Guideline No. 14 29

Glossary 30

Bibliography 43

INTRODUCTION

These Guidelines for Best Practices in E-Discovery in New York State and Federal Courts (the "Guidelines") are intended to provide New York practitioners with practical, concise advice in managing electronic discovery ("e-discovery") issues in both state and federal courts in New York, and to be a reference for best practices in e-discovery based on the current state of the law. These Guidelines are not intended to be a comprehensive review of e-discovery matters or the law of e-discovery. Nor do these Guidelines propose how the law on e-discovery should be changed, or suggest how applicable rules or statutes should be amended. Many excellent resources on e-discovery are available and they are listed in the attached bibliography. Moreover, e-discovery analyses are inherently fact-driven and the Guidelines may not apply, in whole or in part, to any particular case or situation.

Computers are not new to the legal process, and astonishment at the constant and continuous proliferation of electronically stored information (referred to by the acronym "ESI"), networks, systems and devices has become a cliché. However, new developments in modalities of ESI are potentially significant to attorneys because any information relevant to a legal proceeding brings with it concomitant legal obligations. Whether ESI is stored on Facebook, in an iPad, or in the "cloud," counsel must understand the implications for attendant legal duties—such as preservation, collection, and production. Lawyers need not become computer experts; but they do need sufficient knowledge to represent clients competently in a world where "e-discovery" is fast becoming standard "discovery."

Do not make assumptions! Never has this precept been more apt than in e-discovery. There is no exemption from legal duties based on the electronic source of the relevant information. A recorded conversation may not escape preservation obligations simply because it occurred by instant messaging. Lawyers should also never assume, *inter alia*, that:

> the client's Information Technology personnel or the individuals responsible for the client's computer system understand what lawyers say about e-discovery;
> clients understand all of their legal obligations with respect to ESI and will take appropriate steps to carry them out;
> the court will appreciate the difficulties presented by the client's IT architecture;
> the adversary will pay for expensive e-discovery-related costs;
> the vendor will communicate promptly or accurately about any problems or delays in handling the client's electronic information; or
> the adversary will produce ESI in the form your client needs or wants, or in the form in which your client will produce its ESI.

These Guidelines in large part describe electronic discovery practices more relevant to corporate business enterprises with significant volumes of ESI than to small businesses and individuals with more limited resources. Larger business enterprises tend to have correspondingly larger volumes of ESI and more complex variations of electronic systems. However, even companies with access to substantial legal budgets routinely make decisions based on reasonableness and proportionality about how to conduct e-discovery in any particular

case. Smaller businesses and individuals with more limited resources may face a different cost/benefit calculus. But the most cost effective methods of conducting e-discovery may be following the steps outlined in these Guidelines, within a certain scope and budgetary limits clearly defined at the beginning of the case and agreed to by counsel and/or sanctioned by the court.

These Guidelines should help the practitioner recognize certain e-discovery issues that may require further examination and consideration, as well as provide a high-level framework for analysis. The topics addressed represent areas of high risk for client and counsel. The e-discovery case law demonstrates that much, if not most, of this risk arises from a lack of awareness and/or failure to communicate. These Guidelines aim to improve awareness and foster communication, with the goal of containing risk.

GUIDELINE NO. 1: The law defining when a pre-litigation duty to preserve ESI arises is not clear. The duty to preserve arises, not only when a client receives notice of litigation or a claim or cause of action, but it may also arise when a client reasonably anticipates litigation or knew or should have known that information may be relevant to a future litigation.

Comments: There is no specific provision in the Federal Rules of Civil Procedures, the New York Civil Practice Law and Rules, or any other applicable procedural rules defining when any pre-litigation duty to preserve is triggered. The duty to preserve evidence may arise from other statutes or regulations or the common law, as defined in case law. Federal case law illustrates a wide variety of triggers, from the common (*e.g.*, a credible litigation threat letter from a lawyer) to the more controversial (*e.g.*, lawsuits alleging product defects filed against other businesses in the same industry). New York State courts have addressed the duty to preserve primarily in the context of sanctions for spoliation. There are no bright line rules defining with specificity the point at which the preservation obligation is "triggered." It would be challenging to describe comprehensively the possible scenarios that might act as a "trigger" of the duty to preserve ESI. Moreover, efforts to define with specificity what events "trigger" the duty to preserve may not account for particular facts and circumstances specific to individual cases.

It is settled, under New York law, that a client must preserve evidence when that client has notice of pending litigation, or when a client has notice that the evidence probably will be needed for future litigation, or when a client must retain evidence pursuant to regulatory requirements. But it is far from clear what a client's obligations are before clear notice of a pending claim appears. Some New York courts have looked to the standards applied by the New York federal courts for guidance as to when the duty to preserve attaches.

Despite the seeming lack of clarity in the case law as to what events trigger the duty to preserve, general conclusions may be drawn. The legal duty to preserve relevant information arises when a legal proceeding is reasonably anticipated. Circumstances other than suing or being sued may also give rise to preservation duties, such as a regulatory investigation, a non-party subpoena, or a regulation requiring retention of information. Participation in a legal process where production of ESI may be required could also trigger the preservation obligation. Accordingly, the actual filing of a lawsuit or receipt of a subpoena may be the *latest* possible point triggering the preservation obligation. When a client receives notice of litigation or a claim regarding which the client holds relevant information, the preservation duty may be triggered, regardless of what documents have or have not been filed with a court, or formally served.

Given that reasonable minds may differ on when litigation is reasonably anticipated, especially with the benefit of 20/20 hindsight, the better practice often is to take a conservative approach. If there is real doubt as to whether the duty to preserve has been triggered, the safer approach usually is to assume that the duty might exist. While this may be the safest approach from a risk avoidance perspective, it is not always the most practical in light of a balancing of risk and cost.

In determining whether facts may have triggered the preservation obligation, the first step is to assess whether a legal hold concerning ESI (*i.e.*, the process implementing compliance with the duty to preserve) should be initiated. This is a judgment call made by counsel based on all

available facts and circumstances. Client organizations need to advise their employees (and/or outside advisors) designated to determine whether a preservation obligation has been triggered of the existence of the relevant facts and circumstances. Organizations may consider establishing procedures to ensure that such reporting occurs. In contemplating the potential need to justify at a later date the decision to implement, or not implement, a legal hold, the supporting rationale for the decision should be documented in writing in a manner that preserves applicable legal privileges. These decisions may not be questioned, if at all, until years later, perhaps following changes in personnel such as in-house counsel, so avoiding a 20/20 hindsight judgment that is unrealistic given the contemporaneous context that led to the decisions is critical. It is important that a written explanation is drafted and retained that justifies the decision and discusses all the facts and circumstances known at the time the decision was made and on which the client and counsel relied in determining whether there was, or was not, a reasonable anticipation of litigation.

GUIDELINE NO. 2: In determining what ESI should be preserved, clients should consider: the facts upon which the triggering event is based and the subject matter of the triggering event; whether the ESI is relevant to that event; the expense and burden incurred in preserving the ESI; and whether the loss of the ESI would be prejudicial to an opposing party.

Comments: Once a decision has been made that a duty to preserve has been triggered, the scope of that duty must be evaluated. As indicated above with respect to triggering the preservation duty, the determination of scope of preservation is a legal judgment that must be based on all of the available facts and circumstances. For the same reasons as discussed above, decisions about scope should be documented along with supporting reasoning in a manner that preserves applicable legal privileges.

Decisions as to scope may address time frames, custodians, subject matter, and responsive information by source or system, category, or type. Keyword searching and other tools may be available to identify ESI deemed to be within the scope of the preservation duty. Factual investigation including interviews of key witnesses may be indicated. As with the determination of the trigger point, it is often best to be conservative and preserve broadly. You can always argue about the appropriate boundaries of discovery later, but if you fail to preserve ESI and the court decides you should produce it, you will have a serious problem.

Identifying key witnesses and custodians early in the process is essential to effective preservation and discovery. Where it is difficult to identify particular individual custodians, it may be necessary to conduct preservation based on an analysis of what departments, regional offices, or other organizational subdivisions might include custodians believed to possess relevant information. In addition to specific individuals, entire departments or divisions may be deemed responsible for subject matters, such as contracts or specific projects that are the subject of a dispute or investigation. In identifying custodians, it is important to consider former employees, independent contractors, and any other individuals who may have had access to relevant information, and take reasonable steps to preserve relevant ESI on the desktops, laptops and files of former employees and independent contractors, to the extent the ESI is available as of the trigger point.

<u>GUIDELINE NO. 3</u>: Legal hold notices will vary based on the facts and circumstances but the case law suggests that, in general, they should be in writing, concise and clear, and should include: a description of the subject matter; the date ranges of the ESI to be preserved; a statement that all ESI, regardless of location or storage medium, should be preserved unless other written instructions are given; instructions on how to preserve the ESI and/or whom to contact regarding how ESI is preserved; and the name of a person to contact, if questions arise. Counsel should monitor compliance with the legal hold at regular intervals.

<u>Comments</u>: A written "legal hold" notice should be issued to the applicable custodians of information to instruct them regarding the duty to preserve and how it relates to information under their control. The goal here is to implement effectively a two-part process: (1) prohibit destruction and (2) monitor preservation efforts. In addition, the Information Technology ("IT") organization must be provided with a list of custodians who are subject to the legal hold to ensure that any routine deletion of ESI from electronic information systems is suspended for the applicable custodians. Where the client does not have an IT department, this responsibility falls on whomever has the practical ability to control the systems. Note that in certain cases, primarily where a large number of custodians are involved, it may be appropriate to issue legal hold notices to managers or supervisors of custodians for further "down the chain" implementation rather than sending a notice to each and every potential custodian.

Legal hold notices often precede the issuance of a written demand for the production of the needed information. While the content of legal hold notices will vary from case to case because they are, by nature, fact specific, they should be consistent where there is no reason for revision. The key to effective legal hold notices is simplicity and clarity because notices that are difficult to understand or take too long for employees to read hinder compliance. Elements of successful legal hold notices include, by way of example: a brief description of the subject matter and date range of the target information; a clear statement that *any* location or medium of storage is included (unless other written instructions are provided); instructions for the custodian to follow to ensure compliance; and a resource to contact with questions.

From a technical point of view, implementing legal holds can be easy or difficult (and everything in between) depending on the nature of the sources and systems that must be addressed. Typical technology issues involved in legal hold implementation include, for example:

1) the importance of timing because of routine operations of information systems that delete information;
2) the viability of sending out and following up on hold notices by email or whether in-person contact is required;
3) tracking the progress of steps to carry out the hold, including notices and systems implementation;
4) the impact of removing backup tapes from the routine recycling, overwriting, or destruction process;
5) the automated implementation of holds across various systems, such as emails, databases, file servers, etc.;

6) whether collection (versus hold-in-place), is the best or most appropriate method of hold implementation under the facts and circumstances presented;
7) stopping "auto-delete" functions; and
8) ensuring that all ESI sources are properly identified and addressed, including online, near-line, and offline servers and storage devices and home computers, when applicable.

Actions to prevent loss or alteration of potential ESI could include preventing manual or automated system operations such as:

1) using any software, hardware, or other means that might cause the overwriting, erasing, alteration, concealment, discarding, or destruction of ESI;
2) disabling any process that might prevent the normal logging of any form of transaction related to any form of ESI;
3) reassigning, altering, or disabling passwords, user authentication, document certificates, or any other form of custodian, user, and ESI identification and access capability; and/or
4) altering or preventing access to any desktop or portable computing or communication device that might contain potential ESI.

Depending on the circumstances, affirmative actions to preserve ESI might include:

1) establishment of a secure repository for housing collected ESI;
2) preservation of archival and backup media;
3) preservation of the content for specified individuals that may be stored on email and file servers, desktop and laptop computers, portable devices, removable media, and in online accounts;
4) forensic imaging and/or removal from service and securely impounding selected computing and storage devices and media related to designated individuals; and/or
5) preservation of tangible items that may be required to access, interpret, or search potentially relevant ESI, including logs, network diagrams, flow charts, instructions, data entry forms, abbreviations, user IDs, passwords, authentication keys, user manuals, and other legacy or proprietary media or devices required to access potential ESI.

It also may be advisable to issue a preservation notice to an adverse party or a potentially adverse party. This decision should be made considering whether the common law duty of the adverse party to preserve has already been triggered, in which case a preservation notice may not be necessary. But where there are legitimate concerns about potential spoliation, sending a preservation notice may be advisable. Such notices should be carefully tailored to ensure that what is being asked of the recipient is not overly broad and unduly burdensome. Clients should expect that sending a preservation notice to its adversary may result in the adversary sending a similar preservation notice to that client. A recipient of such a letter often has a number of difficult judgments to make, including: whether a preservation duty exists, the proper scope of that duty, and whether and how to respond to the letter. Reaching a reasonable agreement with an adversary is the best outcome when the dispute is important. Delimiting the preservation duty

as early as possible with the adverse party and acting in accordance with the agreement substantially reduces the risk of spoliation sanctions later in the case.

Another mechanism available to ensure preservation by an adversary is the preservation order, although this is not frequently imposed. Preservation orders can be a blessing in disguise to a party with a duty to preserve, if the order defines the boundaries of the duty with sufficient specificity. Such an order can reduce the uncertainty that may lead lawyers to advise expensive and operationally disruptive preservation steps. The case law on preservation orders indicates that obtaining such an order requires something more than the existence of a preservation duty -- which exists in every case -- such as a sound basis to believe that spoliation will occur without an order.

Finally, consideration should be given as to whether it is advisable to permit preservation to be controlled by specific custodians if the custodians are personally implicated by the events and/or the company faces significant exposure to liability. High ranking corporate executives may assume that IT will take care of preservation and ignore legal hold notices, and counsel should consider whether the ESI should be physically collected instead. This balancing of cost and risk may suggest that: (i) in criminal cases collection is the right form of preservation; (ii) that where a small and readily identifiable group of custodians holds the key to a multi-million dollar lawsuit, collection should also be used to preserve ESI; or (iii) where the critical data resides on a particular computer, it should be forensically imaged as a means of preservation. Reasonableness, considering all of the facts and circumstances, should guide such decisions.

GUIDELINE NO. 4: Counsel should endeavor to make the discovery process more cooperative and collaborative.

Comments: E-discovery can derail a case and may result in unanticipated, skyrocketing costs if counsel do not cooperate in a manner that may be different than has been the case historically with paper discovery. There is no benefit in trying to "hide the ball" at the preliminary conference or "meet and confer." Incomplete or inaccurate representations inevitably will be revealed later in the e-discovery process. There already have been cases in which counsel's overly optimistic projections as to scheduling and production, based on incomplete knowledge regarding the client's ESI, have cost the client millions of dollars.

A failure to be forthcoming about ESI issues could lead to further discovery, ramping up costs and possibly revealing vulnerabilities. In federal court, Rule 30(b)(6) depositions are frequently permitted, and depositions may be noticed in state court actions as well, so that counsel may explore an opposing party's IT environment, retention policies, e-discovery compliance procedures, etc. Such discovery may be avoided if relevant information regarding the client's ESI and computer systems is provided at the outset of the case. This is the type of cooperation that is necessary if the discovery process is to proceed efficiently. If the case gets bogged down in "discovery about discovery," clients will inevitably suffer additional cost and delay. It may be necessary for counsel to explain to the client the significance of being forthcoming on e-discovery issues in order to receive the client's full cooperation throughout the e-discovery process.

When errors in what has been represented to opposing counsel and/or the court are discovered, the duty of candor requires prompt correction and disclosure. If that ethical requirement is insufficient motivation, then consider the cases where severe sanctions have been levied for delays in advising the court about e-discovery problems. Courts often view the failure to report knowledge that a prior representation was wrong as equivalent to a misrepresentation.

There is a range of opinions regarding whether it is advisable to include the client's IT personnel or the client representative with the most knowledge of the client's computer system at the "meet and confer" or preliminary conference. While having a knowledgeable IT person present to address questions that may arise, or to explain detailed technical issues may be beneficial, under certain circumstances, lawyers may be uncomfortable with the unpredictability of having a non-lawyer potentially speak for the client on e-discovery issues. In any event, counsel should identify and prepare one or more of the IT personnel or other client representatives who can perform adequately as witnesses to testify as to the computer system and procedures regarding ESI, should the need arise.

The need for cooperation in e-discovery is the subject of the Sedona Conference's "Cooperation Proclamation," which has been supported by many members of the judiciary. E-discovery can be difficult and complicated, and uncooperative behavior between counsel can only serve to make it more so. Because cooperation in e-discovery can facilitate an efficient process, thus reducing costs, most clients should prefer that their counsel adopt a cooperative approach.

GUIDELINE NO. 5: Counsel should be familiar with their client's information technology, sources of ESI, preservation, and scope and form of production, as soon as litigation is anticipated, but in no event later than any "meet and confer" or preliminary conference.

Comments: In most New York State courts and in all federal courts in New York, counsel are required to confer early in the case, not later than at the preliminary conference, regarding e-discovery issues.

The rules in federal court[1] and in the Commercial Divisions of the New York State Supreme Court[2] require counsel to "meet and confer" about e-discovery *prior to* the preliminary conference. In the Commercial Divisions of the New York State Supreme Court, the parties must consider in advance the following e-discovery issues:

a) preservation of ESI;
b) "identification" of relevant ESI;
c) scope of e-discovery;
d) form of production;
e) anticipated costs and proposed allocation of same;
f) disclosure of the "programs and manner" in which the ESI is stored;
g) identification of systems holding relevant ESI; and
h) identification of the individuals responsible for ESI preservation.

In federal court, the discussions about e-discovery prior to the preliminary conference encompass similar scope and breadth, with the additional requirement of discussing the manner in which inadvertent production of privileged information will be handled procedurally.

In the New York State Supreme Court (outside the Commercial Divisions) and County Court, there is no specific rule obligating counsel to confer *before* the preliminary conference. But if a preliminary conference is held, and when it is deemed "appropriate" by the court, counsel must discuss the above issues at the preliminary conference.[3] Further, if a case "is reasonably likely to include electronic discovery," at the preliminary conference, counsel "must be sufficiently versed in matters relating to their clients' technological systems to discuss competently all issues relating to electronic discovery."[4]

Counsel should check the Rules of each Commercial Division[5] in New York State Court, as

---

1 Fed. R. Civ. P. 26(f).

2 22 N.Y. Comp. Codes R. & R. §§ 202.70(g), Rules 8(a) and (b).

3 *See* 22 N.Y. Comp. Codes R. & R. § 202.12(c)(3).

4 *See* 22 N.Y. Comp. Codes R. & R. § 202.12(b).

5 For example, the New York State Commercial Division for Nassau County has its own "Guidelines for Discovery of Electronically Stored Information ("ESI")" and a Preliminary Conference Order form, which addresses e-discovery issues. *See* Commercial Division, Nassau County, "Guidelines for Discovery of Electronically Stored Information"; Preliminary Conference Order. The Nassau County Guidelines contain many of the requirements relating to e-discovery provided for in the Federal Rules of Civil Procedure.

applicable, as well as the rules of the individual federal judge and the Practice Rules of the particular New York State Court justice to determine whether any additional rules concerning e-discovery apply in a particular case.

After the preliminary conference is held in any of the above referenced courts, the court may issue an order, which may address e-discovery issues.[6]

It is clear from the plain text of these rules that a significant amount of disclosure is required, at the outset of the case, with respect to the client's information technology system as well as the e-discovery process undertaken by each party from start (preservation of information) to finish (production of documents and information). This places a substantial burden on counsel, early in the case, to prepare by assembling accurate information with the client's participation -- a process that is often much more difficult than it might seem initially. The reality is that very few clients have the up-to-date information counsel will need about each potential source of ESI in coherent written form that is easily accessed. In representing individuals and smaller companies without IT departments, the task may be even more challenging and may require more input from the client. Sometimes counsel will also need access to one or more IT personnel who can answer essential questions, but often the required information may be dispersed among many individuals in charge of various aspects of the client's IT system.

The fact that such disclosures will be necessary in any case pending in any of the New York federal courts and many cases pending in the New York State Courts indicates that it is prudent for counsel to work with the client, where appropriate, to prepare the background IT information, if possible, *before* litigation begins. The goal of this effort would be to create a summary of the sources of ESI and the facts relevant to e-discovery, such as retention periods and format of ESI,[7] which can then be used as a basis for lawyers and client representatives knowledgeable about the client's computer system to begin discussions about e-discovery strategy.

Counsel must also estimate the scope of e-discovery at a time when it may be pure guesswork to do so. The ability to estimate the likely duration of the process as well as its cost is a function of many factors, including the facts of the case, the amount at issue, the adversary and its counsel, the scope of planned e-discovery, the client's IT systems, and the client's budget and resources. Nevertheless, e-discovery is not new, and there is a wealth of informative resources available to assist in projecting e-discovery timelines and cost. In any event, this preparation is essential to fulfilling the mandate of cooperation indicated by the applicable rules.

---

[6] Fed. R. Civ. P. 16(b)(3)(B)(iii); 22 N.Y. Comp. Codes R. & R. §§ 202.12(b); 202.70(g), Rules 8(a) and (b); 11(c).

[7] This type of systems overview is preferable to what is typically referred to as a data map, which is usually a "pictorial" rendering of a network or some other portion of an IT architecture. These kinds of data maps can be incomplete and in any event may be incomprehensible to lawyers.

GUIDELINE NO. 6: To the extent possible, requests for the production of ESI and subpoenas seeking ESI should, with as much particularity as possible, identify the type of ESI sought, the underlying subject matter of the ESI requested and the relevant time period of the ESI. Objections to requests for ESI should plainly identify the scope and limitations of any responsive production. Boilerplate language which obscures the particular bases for objections and leaves the requesting party with no clear idea of what is or is not being produced should be avoided. If necessary, counsel should meet and confer to resolve any outstanding disputes about the scope or format of production.

Comments: Written document requests for ESI and subpoenas for ESI are frequently met with objections that the requests are burdensome and overly broad. In addition, in e-discovery, technical, highly complex issues may render requests inherently ambiguous and compliance very difficult. To avoid, or contain, potential problems arising as a result of these issues, document requests and subpoenas for the production of ESI, and objections to those document requests and subpoenas, should be written in plain, clear language with as much specificity as possible under the circumstances. Accurate communication is key.

In articulating requests for ESI and objections to those requests, there is no place for boilerplate verbiage that is used solely for gamesmanship. Such language may give the party receiving the request the impression that the requesting party wants all ESI ever created. When the responding party uses such language in objections, the requesting party may be left with no idea what the responding party is willing or able to produce, or not produce. If the objections contain this boilerplate verbiage, the requesting party may be unable to discern with any specificity the putative justification for the responding party's objection.

The information needed to tailor document requests to seek information relevant to the claims, causes of action, and defenses at issue in the case should be part of what the parties discuss when they "meet and confer" regarding ESI prior to or at the preliminary conference, as required in all federal courts, and the New York State Supreme and County courts.[8] However, in practice, parties often fail to confer about ESI early in the case, as they should, and in any event cases evolve as counsel gather more information regarding their respective claims, causes of action, and defenses. If you cannot appropriately describe the ESI that you seek when you draft a written request for the production of documents, it is almost always beneficial to pick up the phone and confer with your adversary in an attempt to ascertain what types of ESI the adversary maintains, where the information is located, how it is stored, who the relevant individuals are and any other facts that would assist in specifying the ESI relevant to the claims, causes of action, and defenses in the action.

There may be instances in which a broad request may be appropriate. In such situations, requesting counsel should confer with responding counsel to gather facts to state the request or objection with as much particularity as possible. Conferences among counsel may not always be successful in this regard, so this Guideline is prefaced with the words "[t]o the extent possible."

---

[8] Counsel should check the local rules of each court and the rules of each jurist for any specific additional requirements in this area.

To the extent such lack of clarity may affect fundamental aspects of the production, such as issues relating to form or scope, which may affect costs, and no agreement is reached, counsel should consider seeking judicial intervention before producing ESI. Otherwise, there is a risk that, after production, the court could order the client to search, collect and produce additional or different ESI, which may increase costs and waste time.

GUIDELINE NO. 7: Counsel should agree on the form of production of ESI for all parties prior to producing ESI. In cases in which counsel cannot agree, counsel should clearly identify their respective client's preferred form of production of ESI as early in the case as possible and should consider seeking judicial intervention to order the form of production before producing ESI. In requests for production of documents or subpoenas and objections to requests to produce or subpoenas, the form of production of responsive ESI should be clearly stated. If the parties have previously agreed to the form of production, the agreement and the form should be stated. In any event, counsel should not choose a form of production based on its lack of utility to opposing counsel.

Comments: Form of production is one of the topics specifically identified as a required subject matter for parties to discuss prior to the preliminary conference in Rule 26(f) of the FRCP and Rule 8 of the New York State Commercial Division Rules. It is also an issue to be considered at a preliminary conference, "where the court deems appropriate," in civil actions in New York State Supreme Courts (outside the Commercial Division) and County Courts. If the form of production is not completely resolved or agreed to prior to or at the preliminary conference, the Federal Rules give parties the opportunity to address the form of production in the requests for production of ESI, or the opportunity to object to such form of production in the objections to those requests.[9] In federal court, if there is no agreement to form of production, then ESI must be produced in the form in which it is "ordinarily maintained" or in a form that is "reasonably usable."[10] New York State procedural rules do not provide counsel with similar guidance. Nevertheless, in any case involving ESI, including cases pending in New York State Court, the parties should attempt to agree to the form of production, or identify their preferred form of production, before producing ESI or requesting that their adversary produce ESI.

Failing to identify the form of production could have disastrous results. Counsel may require, where appropriate, that ESI produced by their adversary should be searchable, either full text or with respect to certain categories such as date, author or recipient, to facilitate the use of the ESI. The ESI produced by the adversary should be compatible with the requesting party's computer system or platform. Imagine receiving the electronic equivalent of a million pages of documents only to find that the production is not searchable electronically on your client's computer system or platform. Counsel using document review applications must make sure that the format they request or agree to is compatible with their system and that they request whatever associated information (*e.g.*, a "load file") is necessary to facilitate electronic review. The client should understand the issues involved in choosing the form of production and the client, or its technical personnel, if any and if appropriate under the circumstances, should be involved in the decision.

The choice of production to be used in any given case is a fact-specific inquiry that depends on the form in which the ESI is stored, the parties' respective computer systems, the

---

[9] If a party responding to a request for the production of ESI does not like the form of production requested, it has the opportunity to object and propose an alternative form. If it fails to do so, then it will effectively have waived its right to choose the form of production.

[10] FRCP 34(b)(1)(C); 34(b)(2)(D) and (E).

platform to be used to search the ESI, and other relevant facts. There is no general requirement that ESI must be produced in native format, although many parties insist on that form of production.[11] Producing ESI in native files may not be necessary or appropriate considering the type of ESI requested and/or the issues in the case. Where appropriate, consideration should be given to requiring the production of ESI in native format only as to specific categories of ESI. Moreover, native files present problems relating to Bates Stamping and affixing other kinds of notation directly on files because affixing a Bates number or other designation on a native file will alter the native file. These issues may sound like minor irritations, but as the parties start to take depositions and want to show exhibits to witnesses, identifying and verifying the authenticity of the exhibits can become difficult when using ESI in native format.

It is important to ensure that the form of production demanded or agreed to does not require your client to transform native ESI in a way that is unreasonably expensive. Certain specialized or custom systems may present problems in producing ESI in certain forms. As with most other e-discovery issues, careful consultation with the client's IT personnel and, in some cases, outside experts is critical before reaching agreement on the form of production.

In determining the form of production, parties should also consider whether they want to request the production of metadata and, if so, what metadata to request.[12] Requests for metadata, like all requests for ESI, must be relevant. Requesting "all metadata" is almost certainly overbroad, as programs may generate many kinds of metadata that could not possibly be relevant to a lawsuit. Any request for metadata should be specific enough so that the requesting party can demonstrate why each field or type of metadata is relevant to the case. In determining what metadata should be requested from the adversary or produced to an adversary, counsel should consider: (i) the ability to search by authors, recipients and text, as necessary to identify certain subject matters and to be able to segregate potentially privileged ESI which was authored by, sent to, or refers to in-house or outside counsel or discusses legal advice; (ii) whether the court requires an index of ESI as it corresponds to the requests, and (iii) the list of major players involved in the case, and other similar issues.

In practice, it is common for parties to produce certain ESI in native file format along with image files (such as TIFF or .pdf) and searchable text, along with searchable metadata fields. For example, metadata relating to the date, the author, the recipient, and other aspects of the information may be produced by both parties.

---

[11] Please see the definitions of Native Files and Metadata in the Glossary.

[12] It is not necessary to receive native files in order to receive metadata. Metadata can be extracted and provided along with the related file in other, more manageable formats.

GUIDELINE NO. 8: Producing ESI should be conducted in a series of steps, as follows: (1) initial review; (2) search for and collection of ESI; (3) processing of ESI to eliminate duplicates and render it searchable; (4) culling the ESI to reduce volume; (5) review by counsel; and (6) production.

Comments: To be achieved cost-effectively, electronic discovery must be conducted in an orderly manner. Described below is a process typical of many cases in which substantial e-discovery is undertaken:

(1) The first phase usually involves a high-level, initial review of emails and other ESI associated with key witnesses. In cases involving a large volume of ESI, this may be accomplished by taking random samples or by targeting a particularly important but relatively narrow time period. The potential cost of the process may be roughly estimated by considering the expected volume of ESI that will need to be searched and reviewed, as well as the sources from which that ESI will need to be collected. This phase may also involve initial conferences with opposing counsel, including the "meet and confer" required by the rules of certain courts, to discuss the scope of preservation and discovery and the form of production. Clients that are smaller businesses or individuals, or clients in small cases who may choose to have limited budgets for legal fees and e-discovery, should pay particular attention to agreeing with opposing counsel to the scope and form of production to avoid incurring unnecessary expense regarding searching, production and the form of production. They should also seek to agree with their adversary as often as possible to avoid costly e-discovery disputes and costly e-discovery do-overs.

(2) The second phase includes the search for and collection of relevant ESI. If the parties identified an initial "scope of discovery" during the "meet and confer," then that would form the basis for the execution of initial searches across all sources of potentially relevant ESI. Searches are designed to filter information according to a variety of parameters that are relevant to the matter, including, for example, key words or phrases, key persons, and dates. To the extent possible, counsel should seek to agree with opposing counsel as to the searches conducted, the types of ESI searched and the time period of the search. This process often occurs in multiple stages as more is learned about what is in the documents and how best to identify what is relevant.[13] Ideally, ESI collected from identified sources would be placed in a central repository or platform which provides security, protection, and access by authorized parties.

(3) The third phase is data processing. The purpose of processing is to decompress files, extract metadata from files, eliminate duplication ("deduplication"), and prepare the collected information for loading into a document review software tool so that the information may be searched and reviewed by counsel. This process may include creating image files such as TIFF or PDF and text files from scanned images using OCR software.

13 Electronic searches may not be possible prior to collection and/or processing. The extent of electronic searching that is possible at this stage depends on what tools are available and what sources of ESI need to be searched. Thorough electronic searching may have to wait until a broad scope of ESI is collected and/or processed, after which ESI can be loaded into a review tool that allows robust searching of the processed ESI.

(4) After processing, further trimming of the data, sometimes called "culling," is usually required. This process involves more refined searches, filtering, and queries used to reduce the volume of ESI and create a set of potentially responsive documents for detailed review. The reality is that culling can take place at various points in the process as additional information is acquired that allows counsel to "zero in" on a more precise set of data relevant to the matter.

(5) The fifth step, universally acknowledged as the most expensive part of the process, is review by counsel. In preparation for the review, the information is organized so that it can be reviewed by counsel in an efficient, cost-effective manner. Counsel use a variety of document review software tools or "review platforms" to facilitate the review process. Documents for review are uploaded to the respective document review platform. The review platform enables counsel to perform various functions, such as native file analysis, redaction, annotation, and privilege review, and enables counsel to group or tag documents by designated categories, such as "Hot" documents, privileged, "further review", or other categories tied to the specific facts of the case or the document requests.

(6) Finally, the relevant, responsive, non-privileged ESI is prepared for production. Most litigation support systems leave the original files intact, but convert the files to TIFF or PDF while applying the appropriate redactions of privileged or confidential information, and adding annotation, Bates stamps, headers, and footers. The pages may be printed or stored on a hard drive in a folder structure. The collection of files typically is placed on a CD, DVD, or USB hard drive for production or presentation.

GUIDELINE NO. 9: Parties should carefully evaluate how to collect ESI because certain methods of collection may inadvertently alter, damage, or destroy ESI. In considering various methods of collecting ESI, parties should balance the costs of collection with the risk of altering, damaging, or destroying ESI and the effect that may have on the lawsuit.

Comments: In e-discovery, computer forensics relates to the science and art of examining and retrieving ESI from computers and other electronic devices and their associated storage devices, as well as the Internet, using methods validated by legal authorities and designed to facilitate the admissibility of evidence. In many cases, conducting e-discovery requires special handling where there is risk of ESI being inadvertently or purposefully altered or destroyed, or because certain ESI can only be extracted using special forensics techniques. In addition, in certain cases it is preferable to use an independent expert to avoid questions about whether self-interested parties may have affected the results.

Contents of storage media may be compromised because the media has degraded or has been damaged, or because some or all of the content has been deleted accidentally or intentionally by reformatting, repartitioning, reimaging, or using specialized software to perform thorough overwrites. Metadata may be altered by the simple act of moving a file to a new location, as is routinely done using common copying utilities.

To the dismay of many users, most computers do not remove the contents of a file when it is deleted, either when deleted manually by users or automatically by the system. In most operating systems, the contents of the file remain on the storage medium, while information about the file is removed from the file system directory. In some systems, even much of the metadata remains. ESI will remain on the storage medium until the operating system reuses (overwrites) the space for new data. Even when extreme attempts have been made to delete content, or the storage media has been severely damaged, forensics experts have been able to recover substantial evidence.

An exact copy of a system and all its ESI might be considered an ideal situation for e-discovery practitioners, but is impossible in conditions under which most companies must operate. Consequently, most ESI resides in systems undergoing automatic operations that can potentially disturb relevant information. In addition, normal user operations such as opening files, copying files, sending and receiving files, or turning a computer on or off can compromise the metadata of an electronic document.

Forensic experts and e-discovery practitioners are guided in any particular ESI acquisition situation by the circumstances and requirements of that particular situation, such as agreements reached among the parties, relevance and importance of ESI, cost and time constraints, potential business interruption issues, and claims of privilege. Aside from these circumstances and requirements, forensic experts and e-discovery practitioners need to be able to represent that they have taken all reasonable steps to ensure that all captured content has been preserved unaltered.

It is critical to document each step in the acquisition of ESI, to respond to challenges or inquiries as well as to support admissibility.

It is possible that some potential sources of ESI are disregarded simply because employees believe that potentially relevant content has been deleted or that the storage medium has been damaged, is degraded, or is otherwise not accessible for other technical reasons. However, because of the possibility that employees or witnesses may not have considered all of the technical factors, and because of the demonstrated success of forensics experts, thorough inquiry should be made with respect to all media (including information acquired via the Internet).

Because of budget or other constraints, some clients may prefer to perform computer forensics using internal IT staff familiar with information or network security. There are some important issues to consider before doing so. IT staff may not have the kind of in-depth knowledge, experience, or tools appropriate to perform computer forensics in an e-discovery context. Handling ESI for purposes of legal proceedings is a specialized field with specialized technology. IT staff may also not have the time to conduct e-discovery given their other commitments to ensure the IT operations of the business. In addition, they are not independent, and accordingly the original evidence is being handled by a party with an interest in its contents and its relation to the outcome of the litigation.

Organizations seeking to handle collections internally will need to devote significant resources to training and dedicating personnel to perform computer forensics. A significant investment will also be required in the software and hardware tools necessary to handle ESI properly from an evidentiary standpoint. Nevertheless, in many civil litigations, less expensive methods of collection may be perfectly acceptable. Lawyers and their clients need to assess their appetite for risk based on the adversary, the nature of the threat, and the potential exposure to the business in terms of reputation and monetary liability.

GUIDELINE NO. 10: Parties may identify relevant ESI by using technology tools to conduct searches of their ESI. In most cases, parties may search reasonably accessible sources of ESI, which includes primarily active data, although if certain relevant ESI is likely to be found only in less readily accessible sources or if other special circumstances exist, less readily accessible sources may also need to be searched. The steps taken in conducting the search and the rationale for each step should be documented so that, if necessary, the party may demonstrate the reasonableness of its search techniques. Counsel should consider entering into an agreement with opposing counsel, if appropriate, regarding the scope of the search and the search terms.

Comments: Search is an iterative process in the effective execution of e-discovery, including the process of identifying and reviewing ESI for relevance, privilege and other reasons. It is the key means of reducing the substantial volume of ESI to a smaller set of relevant, responsive and producible information and documents.

As a general matter, counsel should search for ESI in those sources most likely to contain relevant information and the scope of the search should be reasonable, considering the circumstances of the case and the client's computer systems and document retention policies. Sources may include, among many other things, desk tops, laptops, hard drives, servers, home computers, handheld devices, removable media, such as CDs, DVDs and flash drives, and sources of voice mail. Initially, the search for relevant ESI should be conducted from current data files. However, where other sources contain non-cumulative and relevant ESI, they may also need to be searched. For example, if the party has reason to believe that certain relevant ESI may *only* be located in a less readily accessible source, such as backup tapes, then that client may need to search the tapes. In the ordinary case, unless the opposing party shows good cause why ESI from sources that are particularly burdensome to access should be produced, and the court orders the party to produce ESI from such sources, at least as an initial matter, the party need not search those sources.

In most cases, if one party requests the other to search sources that are disproportionately burdensome to search under the circumstances, the searching party should consider requesting that the costs of such a search be allocated or shared among the parties. In requesting that opposing counsel search less accessible sources, counsel should be prepared to receive a reciprocal type of request from opposing counsel to produce additional ESI from less accessible sources, depending on the facts of the case. In determining whether a review of ESI from less accessible sources is justified under the circumstances, counsel should weigh the cost and other burdens incurred in searching less accessible sources against the likelihood of finding relevant evidence.

Because of the complexity of most IT infrastructures and the massive volume of potential ESI frequently encountered in complex cases, the most effective way to perform a search is through application of automated tools. Search software tools provide techniques that enable reduction of ESI based on selected criteria. However, lawyers must understand the limitations of search tools if they are to be confident that they have identified all of the documents and information they are required to produce. There are always sources of ESI or types of files that

search tools may not be able to reach effectively, and there are often search parameters that search tools cannot execute or may not execute depending on the form of the ESI. Counsel should stay informed as to the most current search tools available, as new developments in technology may affect the cost of searches and therefore the cost of e-discovery.

There are a number of considerations related to conducting searches, including the scope of the search, the objectives of the person performing the search, the search criteria used, the capabilities of the software, and the interpretations of the results of the search. The legal team should work with someone thoroughly knowledgeable about the search protocols and tools and their application to the sources under consideration in conducting the search. The various aspects of the search should be documented, with an explanation as to why each step was taken (or not taken). It may be necessary later in the legal process to provide affidavits certifying the accuracy and comprehensiveness of the search methods used and/or explaining the search methods.

The most common approach to searching is through the use of keywords. This is a simple method in which a person enters selected words into a text field of the search program, the search program searches through a list of documents or ESI, and returns a list of the ESI containing the search terms that were entered. Keyword searching can be effective in minimizing the quantity of producible records, which can in turn reduce the cost of generating a review database. Keyword searching identifies documents and ESI in which a search term appears, but cannot determine the relevance of the document to the subject being researched. In addition, keyword searches must rely solely on the specificity of the terms used in the search, and cannot "learn" through use. Because of inherent limitations, keyword searching tends to return more documents than necessary in some situations and fewer in other situations. Consequently, it should be used in conjunction with other search techniques.

There are a variety of search techniques that expand on simple keyword searches to provide more robust and useful results. Some of these techniques are used during the collection of ESI, while others are more appropriate during data processing or review and analysis. A list of common search techniques, including Boolean searches, "clustering" and "concept searching," fuzzy searches and others, are defined in the Glossary.

One common practice is for counsel for both parties to attempt to enter into an agreement regarding the scope of the search and the search terms. In many New York State Courts and in federal court, counsel for both sides are obligated to confer regarding e-discovery issues, and one result of this meet and confer may be a written agreement regarding each party's search process, or a search protocol. In the protocol, counsel may agree to the list of each party's custodians whose desktops (and other sources of ESI), should be searched. If the client's IT infrastructure is organized in a different manner, the parties may agree, for example, which server(s) or platform(s) each party would search. Counsel may further agree to the search terms to be used by each party. Entering into such an agreement may reduce the probability that disputes regarding the search process would develop later.

Decisions regarding the choice of the custodians or servers and the search terms should be documented. This is to enable the party, at a later date, to be able to justify the decisions

made and to be able to explain why the choice of the custodians or servers and search terms was reasonable. Before finally agreeing to search terms or a list of custodians, counsel should conduct a test search to determine whether relevant ESI is likely to be identified by using the proposed search protocol. The list of custodians and/or the search terms may need to be revised and refined before an effective search is achieved. The terms of the effective search should form the basis of the parties' agreement.

Although electronic search techniques and technology can be highly effective and in any event are necessary given the staggering volume of ESI, human error in implementing searches is always possible. Search results, therefore, should be tested after the search has been conducted to verify that the search was complete, accurate, and identified relevant documents. Specifically, the party should verify that some of the relevant documents it has already identified are included in the search results. Flawed searches can create issues potentially harmful to the producing party, including providing a basis for sanctions. Tests of search results should also be documented for later use, if necessary.

GUIDELINE NO. 11: Counsel should conduct searches using technology tools to identify ESI that is subject to the attorney-client privilege, the work product immunity and/or material prepared in anticipation of litigation. Counsel should document its privilege searches and verify the accuracy and thoroughness of the searches by checking for privileged ESI at the beginning of the search process and again at the conclusion of the process. To avoid the situation in which an inadvertent production of privileged ESI may possibly be deemed a waiver of the privilege, counsel should consider, as appropriate, entering into a non-waiver agreement and having the court incorporate that agreement into a court order.

Comments: Once a set of potentially responsive ESI has been identified, counsel should use automated tools and applications in the same manner discussed above to search that set of ESI to identify and withhold, as applicable, any communications subject to the attorney-client privilege, the work product immunity, material prepared in anticipation of litigation and/or any other privileges or immunities that may be involved in the case. In formulating an effective search, counsel should confer with the client and review at least a sampling of the ESI to ascertain, among many other things: (i) the names of all lawyers involved in the underlying facts of the case; (ii) the relevant dates on which the client began to consult with its counsel; (iii) topics of privileged communications; and (iv) any other unique facts relating to the privileged communications. As the ESI is reviewed, additional facts relating to the privilege may be discovered and may require that additional searches be conducted. After all necessary searches are conducted, counsel should check and verify the effectiveness, completeness and accuracy of the searches. Counsel may have to demonstrate to the court at a later date that counsel took reasonable steps to identify privileged communications.

Whether the case is pending in federal court or New York State Court, counsel should consider, as appropriate, entering into a non-waiver agreement with opposing counsel and/or having the court incorporate that agreement into an order, as provided in Federal Rule of Evidence 502. The ever expanding volume of ESI that lawyers must review for privilege may increase the probability that an inadvertent production of privileged information may occur. For this and other reasons, Rule 502 was added to the Federal Rules of Evidence. Rule 502(b) provides that any disclosure of a privileged communication in a case pending in federal court will not "operate as a waiver" if the disclosure was inadvertent, if the client took "reasonable steps" to prevent the disclosure, and if the client promptly took reasonable steps to inform the opposing party of the disclosure and request return of the privileged information. Taking "reasonable steps" may likely include some method of verifying and checking on the effectiveness, completeness, accuracy and quality of the searches for privileged communications. Among other methods, this may involve searching for known privileged communications among the documents to be produced prior to production or conducting other similar checks. Should a privileged communication be inadvertently produced, counsel may have to submit an affidavit to the court explaining the process it used in searching for privileged ESI, including verifying that the searches for privileged information were thorough and accurate, in order to secure a ruling that the production was inadvertent and does not constitute a waiver of the privilege.

In addition, Rule 502(d) and (e) provide that, if the parties enter into an agreement providing that inadvertent production of privileged information shall not constitute a waiver of

the privilege, and the court incorporates that agreement into a court order, that order is binding, not only on the parties to the instant litigation, but also on non-parties in other actions brought in either federal or state court. *See* Fed. R. Evid. 502(d) and (e). The drafters of Rule 502 reasoned that it would be unlikely that parties would actually reduce the costs of their pre-production review of privileged information if the non-waiver agreement or court order referenced in Rule 502 only applied to the instant litigation, and if a non-party could use any inadvertently produced privileged communication against the client in another lawsuit. Therefore, the Rule provides that the inadvertent production does not constitute a waiver of the privilege in the federal court proceeding in which it occurred or in any other action pending in federal or state court (including New York State Court).

There is no equivalent to Rule 502 in New York State Courts. The ethical rules applicable in New York provide that if a lawyer receives a document that may be privileged and the lawyer "knows or reasonably should know that the document was inadvertently sent," the lawyer "shall promptly notify the sender." Rules of Professional Conduct, R. 4.4(b). There is no obligation to refrain from reviewing the information or to return the document. Therefore, in cases pending in New York State Courts, counsel should consider entering into a non-waiver agreement and requesting the court to incorporate the non-waiver agreement into an order, although that order would not be subject to Rule 502(d) and would not be controlling in other actions. A non-waiver agreement or an order would provide protection for an inadvertent production which is not otherwise provided by New York law.

GUIDELINE NO. 12: Counsel should take reasonable steps to contain the costs of e-discovery. To that end, counsel should be knowledgeable of developments in technology regarding searching and producing ESI and should be knowledgeable of the evolving custom and practice in reviewing ESI. Counsel should evaluate whether such technology and/or such practices should be used in an action, considering the volume of ESI, the form of ESI and other relevant factors.

Comments: The volume of ESI involved in preservation and discovery substantially increases the costs of litigation. The lion's share of these costs is incurred during the review phase of e-discovery, when lawyers review ESI to identify relevant information for production, designate privileged information and documents for withholding, categorize information for use in depositions, and otherwise review the ESI. Clients incur additional costs in identifying, searching, preserving, collecting, extracting, loading and preparing ESI for production. These costs can be substantial where the volume of ESI possessed by the client is significant.

The aggregate cost of e-discovery can be most effectively controlled by implementing proactive programs, such as document retention policies, hold and collection procedures, adjustments to IT practices, user education and other measures beyond the scope of these Guidelines. For example, proper implementation of an effective document retention policy pursuant to which a client, in the ordinary course of business when no legal hold is in place, retains only ESI that it needs for business purposes and discards non-useful ESI that it has no obligation to retain, may reduce the volume of ESI in the client's records. This may reduce the cost of searching those records through e-discovery. But in practice, many litigators are contacted by or introduced to a client after litigation is anticipated or has commenced and the duty to preserve ESI has been triggered. Proactive programs involving the deletion of ESI in the ordinary course of business should be suspended once litigation is anticipated or pending.

Technical developments may be used to help reduce the cost of review and improve the accuracy of the review. Computer software, if implemented and effectuated properly, can identify relevant documents as well as, if not better than, human review of each document and may be more accurate and more cost-effective than traditional, manual document review.

Individual clients and small businesses, and clients involved in cases in which the amount in controversy is not substantial, should attempt to contain the costs of e-discovery by attempting to agree with counsel at the preliminary conference to limit e-discovery as much as reasonably possible given the facts and circumstances of the case. For example, the parties may agree to limit the number of custodians whose ESI is produced, the parties may agree to the form of production and the search terms to be used, and the parties may agree to produce ESI, at least initially, only from the most convenient, least expensive and least burdensome sources.

If a client seeks to work with a vendor or if counsel determines that retaining a vendor is necessary to produce, safely and effectively, the volume of ESI involved in the particular case, counsel should proceed with care. The process of "handling" ESI for legal compliance purposes is the subject of ongoing technical research and development, with vendors racing to outdo each other in selling their product's effectiveness and value. Lawyers should be careful not to advise clients regarding a vendor's products without adequate research and experience. In many cases,

consideration should be given to having the client retain the vendor directly. Counsel and vendors should clearly demarcate their respective responsibilities with respect to the production of ESI to achieve cost efficiencies and avoid mistakes.

Research has shown that whether ESI review is performed by humans or by computers, relevant information may be overlooked and not produced, and irrelevant documents may "infect" productions. Thus, lawyers should consider focusing on improving the process used to identify relevant ESI and focusing on testing that will validate the results of the process.

GUIDELINE NO. 13: Parties should discuss the expected costs and potential burdens, if any, presented by e-discovery issues as early in the case as possible. If counsel expects that the client will incur disproportionate, significant costs for e-discovery or that e-discovery will otherwise present a financial burden to the client, counsel should endeavor to enter into an agreement with opposing counsel to allocate the costs of e-discovery or, if necessary, seek a court order as early in the case as possible and before the costs are incurred, allocating the costs of e-discovery and identifying which party pays for what e-discovery costs.

Comments: Issues relating to the sharing or shifting of the costs of e-discovery usually do not arise when both parties to a litigation are of the same size or financial means, or are seeking similar amounts and/or types of ESI. However, when there is a divergence between the parties and one party believes it can demonstrate that it will incur a disproportionate share of the costs of producing ESI, that party: (i) should consider seeking the agreement of opposing counsel to share the e-discovery costs; or (ii) should consider making an application to the court for an order that the costs should be allocated between the parties. It is unlikely that the opposing party would agree to assume additional costs of e-discovery absent a court order, but certain circumstances may result in such an agreement and some courts require counsel to try to resolve discovery disputes with opposing counsel before making an application to the court.

A request for an order allocating costs of e-discovery should be made as early as possible in the litigation, such as at the preliminary conference or at an early status conference or, if necessary, by motion. If possible, the request should be made before such costs are actually incurred. The application may be based on proof of any facts that increase the cost of e-discovery, such as, the excessive cost of review or recovery of ESI which is stored, for instance, on backup tapes, or opposing counsel's overbroad request, or a request for ESI from too many custodians. The moving party may seek an order, for example, directing that e-discovery costs should be allocated or shared by the two parties, or that a portion of the costs should be shifted to the opposing party, or that discovery should be conducted in phases, or tiers, with the production of ESI that is less expensive to produce occurring first, and any additional, more expensive production from other sources occurring only if the opposing party demonstrates it is necessary. The motion should be supported by a detailed analysis of reasons why the moving party should not assume such a financial burden. Where appropriate, consideration should be given to providing an expert affidavit explaining the technical reasons why the e-discovery is so expensive. Counsel should be prepared that a court may not immediately decide the issue of cost shifting and may adopt a "wait and see" approach, by denying the party's application, without prejudice to submitting the application at a later date, such as at the close of discovery, or at or after trial.

The rule regarding the allocation of e-discovery costs is different if the case is pending in federal court versus New York State Court. In federal court, the party producing the ESI generally pays for the cost of production. This general rule is altered if there are special circumstances, a court order or a party agreement. But in New York State Court, as between parties, the CPLR has no rule specifically mandating cost-shifting. Nevertheless, some courts have found that the "New York rule" is that the party requesting the ESI generally pays.

However, decisional authority also exists in New York that each party should bear the cost of its own production.

GUIDELINE NO. 14: Courts may issue sanctions for spoliation, or the intentional or negligent destruction or failure to preserve relevant ESI.

Comments: Courts have ample authority to issue sanctions for spoliation arising from specific rules or broad inherent authority. Moreover, courts have wide latitude to determine the type of sanction for spoliation in any given case -- regardless of whether the spoliator intentionally destroyed evidence or did so through inadvertent negligence. Sanctions for spoliation have included, for example:

> monetary fines against the client and/or counsel, including but not limited to payment of attorneys' fees;
> adverse inference instructions to the jury (*e.g.*, instructing the jury that it may assume that the lost evidence was harmful to the spoliator);
> evidentiary preclusion; and,
> striking a pleading or granting a default judgment against the spoliator.

Typically, courts will weigh the prejudice to the other party and the degree of culpability of the spoliator in determining whether and how to sanction spoliation. For the practitioner, this means that it is critical to go beyond simply establishing spoliation and use any means available to show the relevance of the lost evidence. Given the obvious difficulty in proving the relevance of information that no longer exists, some creativity may be required. The greater the degree of culpability, the less courts are likely to require in terms of showing relevance.

Establishing a sound litigation hold process, as discussed in detail above, is the best way to avoid a spoliation disaster. However, it may also be important in showing good faith if spoliation does occur despite the best laid plans. Conversely, exposing the inadequacies in an adversary's process -- or the lack thereof -- is an effective way to show the court that the spoliator had no regard for ESI preservation.

GLOSSARY[14]

A

Adobe Acrobat—From Adobe Systems Incorporated, Acrobat is the leading program for creating and viewing PDF files—available in a free version and Professional version that enables file conversion, search, tagging, and other functions, and allows use of third-party add-ons.

Application Server—A server dedicated to processing applications, such as, for example, accounting systems. Also see *Server*.

Application Service Provider (ASP)—Third party that provides hosting services for a variety of information processing functions, and within e-Discovery, a portion or all of the functions related to the e-Discovery lifecycle. Also see *Hosting* and *Service Bureau*.

Archival Storage—Long-term storage of essential information under strict environmental and security parameters, but not requiring immediate access.

Attachments—Attachments fit two categories—True Attachments and Physical Attachments. True attachments are created by an author or custodian and referred to in the cover or parent document, such as an email with an attachment for example. Physical attachments are bound, clipped, or stapled without any reference by the author or custodian to the attachment. Also see *Unitization*.

Audio File—A file containing analog or digital sound elements, which can be played (heard) through an output device.

Auditability—The transparency, openness, or receptiveness of a system or process to being examined, with inherent features such as logs that facilitate the examination process.

Audit Log/Trail—Chronological record of selected information such as computer user activity for example that might include logins, logouts, files accessed, actions performed, and communications in and out.

Automated Litigation Support (ALS) Systems—ALS Systems are the application of specialized software programs to facilitate execution of functions within the e-Discovery lifecycle. ALS Systems are considered essential to the effectiveness of performing required functions and achieving objectives within the e-Discovery lifecycle.

B

Backup Storage—Exact copy of ESI stored separately from the original to serve as a source for recovery in the event of a system problem or disaster.

Backup Tape—Magnetic tape used to store backup copies of ESI.

Bates Number—A unique serial number electronically impressed on every page of a document collection. Often used in conjunction with a suffix or prefix to identify the producing party, the case, or other relevant information. Bates numbering was originally done by manually stamping the numbers onto hard copy originals.

Best Practices—Methods generally accepted and promulgated within an industry as being superior over others.

Bibliographical or Objective Coding—Recording objective information, such as date created, author, recipient, and copies, from electronic documents and associating that information with a specific electronic document.

Blowback—A hard copy set of documents printed from digital images, and usually produced in a batch from a coded database that enables automatic sorting and grouping of the documents.

Boolean Search—Use of logical operators such as “and”, “or”, and “not” to include or exclude terms from a search. Also see *Proximity Search*.

---

[14] Reprinted from *ESI Handbook: Sources, Technology and Practice*, written by Adam I. Cohen and Edward Kalbaugh, Wolters Kluwer Publishers, 2009, with permission from Wolters Kluwer Publishers.

Broadband—Designation for communication networks, such a fiber optics, having higher throughput than other networks.

Burn—Copying files to a removable media, usually a CD or DVD.

Byte—Consists of 8 bits as the basic capacity measurement for most computer data, and increases in increments of 1,000 expressed as Kilobyte, Megabyte, Gigabyte, Terabyte, Petabyte, Exabyte, Zettabyte, and Yottabyte. Also see Chapter 5, Overview of File and Storage Systems, for *Table of Storage Capacity*.

C

Cartridge—See *Tape Cartridge.*

Case Management Services—A type of litigation support service to help prepare lawyers, law firms, and legal departments to try a case. Specific services may include interviewing witnesses, document review, and case preparation.

Case Management Software—Litigation collaboration software that helps law firms and third parties prepare for and manage a case.

CD (Compact Disc)—A type of optical disc storage media that includes read only (CD-ROM), write once then read only (CD-R), and write multiple/read multiple (CD-RW).

Certificate—Electronic affidavit vouching for the identity of the transmitter. Also see *PKI Digital Signature.*

Chain-of-Custody—Documentation and testimony regarding the possession, movement, handling, and location of evidence from the time it is obtained to the time it is presented in court; used to prove that evidence has not been altered or tampered with in any way; necessary both to assure admissibility and probative value.

Child—See *Parent/Child.*

CIO—Chief Information Officer.

Clawback Agreement—Agreement between parties to a litigation outlining procedures to protect against waiver of privilege or work product protection due to inadvertent production of documents or information.

Client—Any computing device that requests a service of another computer system. A *Thin Client* is a wired or wireless device that depends on a host for application processing. A *Thick Client* is a wired or wireless device that may request a service of another computer system, but also has its own computing capability.

Cloud Computing—Accessing files or using software through the Internet, generally via a service provider.

CMS—Content Management Systems are collaboration systems used to manage the creation and communication of corporate documents.

Coding—The inclusion of bibliographical information about each document into an automated litigation support program so that an affidavit or list can be produced in compliance with applicable rules. Coding also enables sorting and grouping in line with relevancy and privilege review. Coding usually includes the following basic information: Author, Bates Number, Date, Document title and type, and Recipient.

Coding Manual—Document providing instructions and information related to the coding function performed within the review process of e-Discovery. Also see *Coding*.

Collection—Process of harvesting ESI from various sources for processing and review phases e-Discovery.

Compliance (Management)—Process of adhering to policy, legal, or regulatory requirement.

Compression—Process for reducing the size of files to reduce storage space and bandwidth required for access and transmission.

Computer Forensics—See *Forensics.*

Computer Memory—See *RAM.*

Concept Search—Taking into account the context within which search words appear to ascertain meaning. Also see *Search.*

Contextual Search—Searching ESI whereby the surrounding text is analyzed to determine relevancy. Also see *Search*.

Correlation Search—A statistical method (Latent Semantic Indexing and Analysis) for finding the underlying semantic relationship of terms and their correlation, whereby the presence of one or more terms could confer significance to a document. A common example would be the relationship of words like law, lawyer, attorney, and lawsuit as representative of a shared meaning. Correlation search enables grouping and clustering of ESI into meaningful categories.

CSO—Chief Security Officer.

Culling—Removing documents from collections to be produced or reviewed. Also see *Harvesting*.

Custodian—The owner or person responsible for safekeeping of ESI.

D

Data—For practical purposes, the building blocks of ESI. Technically, data also includes elements that reside in many places within computing and storage devices, not accessible to users, such as program code, for example. Also see *Data Element* and *ESI*.

Data (Database) Administrator—IT person responsible for maintaining databases.

Database—The term database commonly refers to a collection of records and the software (database management system) used to manage user interaction. Technically, a database and a database management system are separate entities. There are a variety of database structures from which ESI is obtained, including Data Warehouse, Dimensional, Flat, Hierarchical, Network, Object, and Relational. (See Chapter 8, Databases, for a definition of each type of database.)

Database Server—A server optimized for database transactions.

Data Element—A combination of characters or bytes referring to one separate piece of information, such as name or address.

Data Sampling—Method of examining a statistically representative portion of ESI to determine how much of a universe of ESI is responsive.

Data Warehouse—Special form of large-scale dimensional database optimized for intensive queries of diverse business data elements analyzed and used to derive business insights and intelligence.

Deduplication—Deduplication is a software or hardware-based process for identifying exact or near-duplicate files within a collection, and only storing the original and any changes to the original. This eliminates file redundancy, reduces storage volume, and reduces the time required in discovery of ESI. Vertical deduplication locates duplicates within the records and information of a single custodian, while horizontal deduplication applies globally across all custodians. Also see *Near Deduplication, Block-level Deduplication*, and *Single Instance Storage*.

Deleted Data/File—ESI residing on media space that has been designated as available for reuse. The deleted ESI remains intact until it is overwritten. Deletion may be automated or manual and intentional or unintentional.

Deliverable—A project management term used to describe a tangible work product.

Digital Fingerprint—Fixed-length hash code that uniquely represents the binary content of a file. Also see *Hash*.

Digital Signature—See *Certificate* and *PKI Digital Signature.*

Directory—A simulated file folder or container used to organize files and directories in a hierarchical or tree-like structure.

Disc Drive—See *Hard Drive.*

Disc Mirroring—Process for protecting ESI by storing an exact copy of ESI on a second storage media during storage of the original ESI. Also see *Mirroring*.

Document Classification—Using a field bibliographical coding to group documents into categories such as correspondence, memo, report, and article for example.

Document Lifecycle—Phases inclusive of the functions to create, communicate, modify, store, retrieve, and destroy.

DoD 5015—Department of Defense standard for records management.

DVD (Digital Video Disc)—A type of optical disc storage media that can be written to and read from. DVDs are faster, have larger capacity, and support more data formats than CDs.

E

e-Discovery—The preparation, preservation, collection, processing, review, and production of evidence in electronic form in response to business, regulatory, or legal requirements. e-Discovery is also sometimes referred to as EDD (Electronic Data Discovery).

e-Discovery Process Lifecycle—Phases inclusive of the functions: Preparation, Search/Collection, Processing, Culling, Review/Analysis, and Production/Presentation.

e-Discovery Readiness Program—The process and initiatives (projects) to ensure adequate preparation for and optimization of the e-Discovery process.

e-Discovery Response Team—Team formed to execute e-Discovery requirements in response to investigation or litigation.

e-Discovery Vault—A secure, central repository for storage of discovered ESI, that is accessible by authorized users.

Email (Electronic Mail)—An electronic messaging system for communicating information and attached documents to one or more parties. Emails consist of addresses, header information, the message body, attachments, and metadata.

Email Administrator—IT person responsible for maintaining email systems.

Email String/Thread—Series of emails linked together by email responses and forwarding, often treated as a single document.

Encryption—A protection process using complex algorithms to render the contents of a message or file unusable or unintelligible to computers or persons not authorized to use/read it.

Encryption Key—A data value that is used to encrypt and decrypt data.

Endorser—A small printer in a scanner that adds a document-control number or other endorsement to each scanned sheet.

ePaper—Electronic version of a document, usually in PDF or TIFF file format.

ESI (Electronically Stored Information)—ESI is the term adopted in Rules 26(a)(1), 33, and 34 of the Rules of Civil Procedure, Amended December 2006, to include any type of information that can be stored electronically, and to acknowledge that electronically stored information is discoverable. It is intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and technological developments.

Exabyte—See *Byte.*

Exchange Server—A server running Microsoft Exchange messaging and collaboration software. It is widely used by enterprises using Microsoft infrastructure solutions. Among other things, Microsoft Exchange manages email, shared calendars, and tasks.

F

File—Collection of ESI stored under a specified name on storage media.

File Conversion—Changing data or a file from one format to another. For example, converting native files from their original source format to an image-based format such as PDF or TIFF.

File Deletion—See *Deleted File.*

File Format/**Extension**—Three characters (usually) following a file name, to designate the type of file, which

defines how it is stored and used. See the Appendix, File Formats Used Worldwide.

File Server—Computing device optimized to store files for access by multiple users.

File System—Combination of software and logical structures used to organize and manage storage and access to ESI on storage media.

File System Metadata—System generated metadata stored externally from the ESI and used by the system to track ESI. Also see *Metadata*.

Filename—Name of a file excluding root drive and directory path information.

Filtering—See *Search.*

Fingerprinting—See *Forensics* and *Hash.*

Flash Drive—See *USB Drive.*

Forensic Capture/Copy—A method of preserving the original state of a physical storage media, and copying the entire contents of the media to preserve files and folders, and all other information on the media, including deleted files, file fragments, metadata, and other data. Forensic capture applies compression and encryption for protection and to guard against allegations of spoliation.

Forensics—The scientific examination and analysis of ESI while residing on storage media or after being retrieved from storage media, in a manner that conforms to legal requirements for evidence collection for use in a court of law.

FRCP (Federal Rules of Civil Procedure)—Rules that govern civil actions brought in U.S. federal district courts. Many states enact similar rules.

Full Text Search—Search of ESI for specific words, numbers, and/or combinations or patterns. Also see *Search*.

Fuzzy Search—Searches allowing and finding close approximations of words, such as misspellings for example, often to overcome errors during OCR scanning. Also see *Search.*

G

Gigabyte (GB)—See *Byte*.

Governance—Formal oversight of and direction to a process or program by one or more senior persons with authority.

H

Hard Disk Drive (HDD) Cartridge—Small, removable device containing a hard disk. Cartridge fits into a docking station connected to computer via USB port.

Hard (Disk) Drive—Storage device consisting of one or more spinning magnetic media platters on which data can be written and erased.

Harvesting—The process of retrieving and collecting ESI from storage devices/media for processing and loading to Automated Litigation Support (ALS) Systems.

Hash—A relatively small, unique number representing the unique digital "fingerprint" of data, resulting from applying a mathematical algorithm to the set of data. The fingerprint may be called hash, hash sum, hash value, or hash code. Used to validate the authenticity and/or integrity of data.

Hosting—Provisioning of applications, storage, and Internet access by a third party.

HTML (HyperText Markup Language)—Document presentation format used on the Internet that applies tags to enable Web browsers to display text and images.

HTTP (HyperText Transfer Protocol)—Underlying protocol used by the Internet to define how messages are formatted and transmitted, and what actions Web servers and browsers should perform in response to various commands.

Hybrid Search—Enables search and analytics of structured and unstructured data from single interface without requiring change in formats. Also see *Search*.

Hyperlink—Underlying code—represented on screen by underlining words or highlighted graphics—within a document that redirects to another location when clicked on by a user. Documents that include hyperlinks to navigate within the document are called HyperText.

I

Identification—One of the first steps in the e-Discovery process, finding discoverable and relevant ESI within various sources.

Image File Formats—Document images can be saved using different file formats, including JPG, GIF, PDF, single-page TIFF, or multi-page TIFF. ALS Systems can usually handle a variety of different formats.

Imaging—See *Scanning.*

Index—A technique used in information systems to enable faster and more efficient search and retrieval of information in files and databases, typically consisting of a separate file or database of key data elements (dates, names, keywords, etc.), parsed from a source, with pointers to the original source.

Information Asset (Source) Management—The inventory and tracking of custodians, and the IT devices and ESI related to them.

Instant Messaging (IM)—Form of electronic communication involving immediate text correspondence between two or more online users.

Internet—Worldwide, publicly accessible series of interconnected computer networks permitting communication among users.

Intranet—Private network that uses Internet-related technologies to provide services internal to an organization or defined infrastructure.

IP (Internet Protocol) Address—Unique address that electronic devices use to identify and communicate with each other on a computer network using the Internet Protocol. Also see *TCP/IP.*

ISP (Internet Service Provider)—Business providing access to the Internet for a fee. ISPs may be a source of ESI evidence through files stored on their servers. Also see *Hosting* and *Service Bureau*.

IT (Information Technology) Infrastructure—The people, processes, hardware, network, and software components collectively used for information processing and management within an organization.

J

Journal—Chronological record of data processing operations. Journals may be used to reconstruct previous or updated versions of a file. In database management systems, journals are records of all stored data items that have values changed as a result of processing and manipulation of the data.

Journaling—Copying of sent and received emails in native format to a secondary storage device for retention or preservation.

JPEG—Compression algorithm commonly used for still images.

K

Keyword Searching—The use of key words and Boolean techniques to search for documents containing relevant information. Also see *Search*.

Kilobyte (KB)—See *Byte*.

L

LAN (Local Area Network)—A group of computers at a single location that are connected via wired or wireless networks. Also see *Network*.

Lead Date—The date of a parent document, or if no parent, the document's own date. Lead date is used in a database as an option to enable chronological sorting of documents by parent, so that any attachments remain in

chronological sequence.

Legacy Data—ESI residing on outmoded or replaced storage devices for which little or no processing capability or knowledge remains within the organization, or which has become too costly to maintain effectively.

Legacy System—Outmoded IT components for which little or no processing capability or knowledge remains within the organization, or which has become too costly to maintain effectively.

Legal (Litigation) Hold—Communication issued as a result of current or reasonably anticipated litigation, audit, legal, or regulatory matter that suspends the normal disposition or processing of ESI. Hold orders or Hold notices may also be referred to Preservation, Suspension, or Freeze orders or notices.

Linking—The ability within an ALS System to connect evidence, transcripts, notes, pleadings, websites, and other documents to each other with hypertext links.

Load File—A data file is a critical deliverable from the scanning/coding function that establishes links between records in a database and the document image files to which each record pertains. Without a correctly structured load file, documents and their respective database records will not be in sync.

Lotus Domino—IBM's enterprise-level server product that hosts Lotus Notes and Web server capabilities.

Lotus Notes—IBM's enterprise-level collaboration suite that provides email, calendars, custom application development, database, and Web services.

LRP (Litigation Response Plan)—Developed to guide e-Discovery process.

M

Maintenance Programs—Applications that run at scheduled intervals according to predefined rules to maintain ESI and IT infrastructure components.

Meet-and-Confer—Meeting between counsels under Rule 26 of FRPC.

Megabyte—See *Byte*.

Metadata—Metadata provides information about other information sources—origins, usage, authenticity, and characteristics that provide additional meaning and context, and accordingly is considered discoverable evidence. Also, vendors may add metadata as a result of processing, most of which is used for process reporting, chain-of-custody, and ESI accountability. See Chapter 6, Native Files and Metadata.

Metadata Comparison—Comparison of specified metadata as the basis for deduplication without regard to content. Also see *Deduplication*.

Metrics—Units of measurement, and specifically within e-Discovery, those discernable units, such as documents, files, etc., that lend themselves to quantification.

Mirror Image—See *Forensic Capture*.

Mirroring—Duplication of ESI for backup or to distribute Internet or network traffic among several servers with identical ESI.

MPEG (1-4)—Various standards applied to compression/decompression of full motion video to digital.

Multimedia—Combinations of video, audio, text, and graphics in digital form.

N

Native Files—The original form in which a document or file is created by a software application. Two good examples are spreadsheets and word processing documents. Native files contain the content that users see, such as text and spreadsheet numbers, and information (metadata) about the document that users normally do not see, such as author and creation date.

Native File Review—A process that requires opening the document in the application in which it was created, or in a special application capable of supporting native file review.

Natural Language Search—Use of plain language without requiring special connectors or precise terminology. Also see *Boolean Search*.

Near Deduplication—Identification, tagging, or grouping files that do not have the same hash values, but are similar with minor differences in content and/or metadata. An example would be the various threads in an email distribution.

Near-Line Data/Storage—Use of offline storage to retrieve information in near real time for online use via robotics moving storage media (tape cartridges or optical discs) from storage library to read/write device. Also see *Offline Data/Storage.*

Network—Two or more computers and other devices connected together for the exchange and sharing of ESI and resources.

Network Administrator—IT person responsible for maintaining networks.

Network Database—See *Database.*

Node—Any device connected to a network.

O

Object Database—See *Database.*

Objective Coding—Manually reviewing a document and completing database fields, such as Bates number, author, recipient, cc, date, title, type, source, characteristics, and keywords. Objective coding, unlike subjective coding, does not require the coder to exercise discretion or be familiar with a particular case in order to correctly code the document. Also see *Coding*.

Offline Data/Storage—ESI storage in a system outside the online network (network in daily use), and only accessible by means of the offline storage system, which usually requires manual intervention. Also see *Near-Line Data/Storage, Online Data/Storage*, and *Storage.*

Online Review—Use of an ALS System by one or more persons to perform one or more of the review functions.

Online Data/Storage—ESI storage in active systems used in day-to-day operations.

Ontology—Collection of categories and their relationships to other categories and to words, and often used to find related documents when given a specific query.

Operating System (OS)—Software that directs the overall activity of a computer, network, or system, enabling all other software programs and applications to operate.

Operational Storage—Storage of information in active use for day-to-day operations. Also see *Online Data/Storage.*

Optical Character Recognition (OCR) and Optical Word Recognition (OWR)—OCR and OWR are computerized processes that generate a searchable text file from a digital image or picture file when it is scanned. As their names imply, OCR recognizes characters, and OWR recognizes words. OCR software compares the shape of letters in the image with its library of fonts and then generates the appropriate digital letter. Accuracy of OCR is largely dependent on the quality of the original document. OWR uses multiple OCR engines and compares results to a built-in dictionary. OWR is more accurate than OCR especially on older or poor-quality originals.

Outlook—Microsoft program that includes email, task management, and a calendar. All data is saved in a single PST file on the user's hard disc drive.

Outsourcing—Outsourcing refers to the shifting of work from one organization to another, including from within an organization in one country to an organization in another country. Within the e-Discovery lifecycle, Coding is the function most generally outsourced to reduce costs. Also see *Service Bureau.*

Overwrite—To manually or automatically record or copy new data over existing data, permanently deleting the original data.

P

Parent/Child—A hierarchical arrangement in which a subordinate entity is the child of a superior entity. An example would be Microsoft's file system tree structure, where one folder is the parent and folders under the parent

are child folders. Also, in e-Discovery, parent refers to the first, or cover, document and child refers to documents attached to the first or cover document.

Parsing—Transforms input text into a data structure suitable for later processing, while capturing the implied hierarchy of the input. Data may be parsed from one source of ESI to another.

Pattern Recognition/Matching—Pattern Recognition technology searches ESI for like patterns and flags, and extracts the pertinent data. Pattern matching technology compares one file's content with another file's content.

PDA (Personal Digital Assistant)—Mobile handheld device containing common applications for organizing schedules and work.

PDF (Portable Document Format)—Software from Adobe Systems Incorporated that converts single or multi-page documents into Adobe's proprietary format that captures the document's original formatting features and enables display across a variety of computer platforms. PDF provides security, navigation tools, search, and other features that facilitate document exchange.

PDF/A—The International Standards Organization (ISO) PDF specification for the long-term preservation of archived documents.

PDF Conversion—Converting documents in another file format to PDF.

Peripheral—Any accessory device attached to a computer, such as a disk drive, printer, modem, or to a network, such as router, or switch.

Petabyte (PB)—See *Byte.*

PKI (Public Key Infrastructure)—A security arrangement that enables computer users without prior contact to be authenticated to each other, and to use the public key information in their public key certificates to encrypt messages to each other.

PKI Digital Signature—A method for providing authentication of any message using the Public Key Infrastructure. A document or file may be digitally signed using the party's private signature key, creating a digital signature that is stored with the document. Anyone can validate the signature on the document using the public key from the digital certificate issued to the signer. Validating the digital signature confirms who signed it, and ensures that no alterations have been made to the document since it was signed.

Presentation Process—Phase of the e-Discovery Lifecycle devoted to developing trial presentations.

Preservation—The process of ensuring retention and protection from destruction or deletion of all potentially relevant ESI. See also *Spoliation*.

Preservation Letter/Notice/Order—See *Legal Hold*.

Print Server—Server dedicated to delivering printing services via the network.

Private Network—A network connected to the Internet but isolated by security measures allowing use of the network only by authorized users.

Privileged ESI—The compilation of ESI identified and logged as responsive and/or relevant, but withheld from production on grounds of privilege.

Privilege Review—Privilege review is often a combination of automated search and filtering combined with reading selected documents to determine and flag those considered privileged and to be excluded from production.

Production ESI—The universe of ESI identified as responsive to requests and not withheld on the grounds of privilege, and exchanged via electronic media. Also see *Quick Peek*.

Production Number—See *Bates Number*.

Production Process—Phase of the e-Discovery Lifecycle devoted to "packaging" relevant ESI for delivery.

Project Management—Formal methodology for managing resources to achieve objectives.

Project Plan—One of the first deliverables under project management—defines project components and how the project will move forward. Also see *Deliverable*.

Proximity Search—For text searches, the ability to look for words or phrases within a prescribed distance of another word or phrase.

PST File Format—Used by the Microsoft Outlook program. Also see *Outlook.*

Q

Quality Control—Formal method of controlling processes to ensure expected results.

Query—Access to a database to retrieve information.

Quick Peek—A production of ESI made available to the opposing party before being reviewed for privilege, confidentiality, or privacy, under stringent guidelines and restrictions to prevent waiver.

R

RAM (Random Access Memory)—Hardware in a computer that retains memory on a short-term basis and stores information while the computer is in use.

Record—Information, regardless of medium or format, that has value to an organization.

Records Management—Human and automated processes related to influencing the lifecycle of records in accord with business, regulatory, and legal purpose.

Redaction—The "blacking out" of information in documents to be produced. Redaction is usually accomplished in an ALS System by overlay so the original document image is not altered. Redactions should be permanent on documents included in final production.

Relational Database—See *Database.*

Relevancy Screening—The review of documents prior to scanning to eliminate irrelevant documents, using search tools that can filter out irrelevant files by criteria such as date range, custodian, folder, or in the case of emails, by date, author, or recipient.

Residual Data—Term generally referring to any information not serving a current useful purpose on a computer or storage media that may be recoverable using forensics techniques.

Restore—The act of transferring ESI from a backup medium to an online system, and possibly recreation of the original hardware and software operating environment.

Review—One of the functions within the e-Discovery lifecycle whereby potentially responsive ESI is examined and evaluated for selection of relevant ESI, including assertion of privilege or confidentiality for example.

ROM (Read Only Memory)—Permanent hardware memory that can be read but not written to or changed, usually on a chip containing firmware (software on a chip) for starting the computer and running certain imbedded system programs.

Rule 26 Automatic Disclosure of ESI—Parties in litigation must provide a copy (or description by category and location) of ESI that will support that party's claims and/or defenses.

Rule 26 Enhanced Meet-and-Confer Requirements—Parties must meet and confer at the outset of the case to discuss their plans and proposals regarding the conduct of the litigation, including any issues relating to preservation, disclosure, or discovery of ESI, including the form in which ESI should be produced and claims of privilege, or protection as trial-preparation material.

Rule 26 Inadvertent Production of Privileged Information—If discovery information is subject to a claim of privilege, or protection as privileged trial-preparation material, the party making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party is required to promptly return, sequester, or destroy the specified information and any copies it has and is not permitted to use or disclose the information until the claim is resolved.

Rule 26 Production of Information "Not Reasonably Accessible"—A party need not provide discovery of ESI from sources that the party identifies as "not reasonably accessible because of undue burden or cost." The party being asked to produce ESI bears the burden of demonstrating the information is not reasonably accessible because of undue burden or cost. Even if that showing is made, the court may nonetheless order discovery from that party if

the requesting party shows good cause.

Rule 33 Production of ESI In Response To Interrogatories—Provides the option to respond to an interrogatory by specifying and producing the business records, including ESI, which contain the answer.

Rule 34 Production of ESI In Response To Requests For Production Of Documents—Requires production of relevant and responsive, non-privileged ESI,.

Rule 37 Safe Harbor Provision—Remedies for a party's failure to respond to, or cooperate in, discovery. Amended Rule 37 provides that, absent exceptional circumstances, a court may not impose Rule 37 sanctions on a party for failing to provide ESI lost as a result of the "routine, good faith operation of an electronic information system."

Rule 45 Subpoena—For third parties to produce designated documents, electronically stored information, or tangible things in that person's possession, custody, or control, or permit the inspection of premises.

S

Safe Harbor—See *Rule 37.*

Sampling—Sampling refers to the process of testing a database or a large volume of ESI for the existence or frequency of relevant information as an aid in determining whether to perform more extensive searches.

Scanning—Converting text and images of a page of a paper document into a computer file as an image, as readable text, or as a combination of both.

Search—The use of various automated methods for identifying and finding potentially relevant ESI.

Search and Collection—A phase of the e-Discovery Lifecycle devoted to finding and acquiring potentially relevant ESI.

Searchable PDF—A PDF document that retains the formatting and looks of the original document, and can be text-searched using Acrobat or third-party search tools.

Server—A computer on a network that contains ESI, applications, or other services shared by multiple users of the network on their client PCs. See Chapter 3, Overview of the Information Technology Infrastructure.

Service Bureau—Company that provides services such as scanning and coding to the litigation market. Also see *ASP*, *Hosting*, and *Outsourcing*.

Situational Assessment—Examination to determine the current state in relation to the desired state, and to uncover any problems related thereto. Usually followed by a gap-impact-risk (GIR) analysis. Also see *GIR Analysis*.

Spoliation—The deliberate or inadvertent modification, loss, or destruction of evidence by a party who has been put on notice of litigation but has failed to take appropriate steps to preserve potentially relevant information.

Steering Committee—A group of stakeholders formed to provide governance and guidance to major programs.

Storage—Placement of information on a storage device for day-to-day use (operational storage) or for disaster recovery (backup storage) or for long-term retention (archival storage).

Storage Device—Any device, such as a disc or tape drive serving as the host for storage media, capable of storing ESI.

Storage Media—A medium for storing ESI, including magnetic tape, discs, CDs, DVDs, and solid state electronics for example.

Structured ESI—Information organized by computer program in a consistent manner to allow manipulation usually via database structures that enable sorting, searching, and reporting for example. Also see *Unstructured ESI*.

Subjective Coding—High-level legal analysis of documents in an ALS System that relates each relevant document to one or more appropriate legal or factual categories or issues as defined by the lead attorney.

Suspension Notice—See *Legal Hold.*

Synchronization—The ability to merge two or more copies of a database together, preserving rather than overwriting the latest changes made in any copy.

System Administrator—IT person responsible for developing and/or maintaining core infrastructure systems, as opposed to business applications.

T

Tape Cartridge—A plastic housing for a tape reel and the preferred mechanism for use in tape-based storage systems.

Tape Drive—A hardware device used to store or backup ESI on a magnetic tape.

Tape Recycling—Process of overwriting tapes with new data, usually on a fixed schedule involving tape rotation.

Tape Restoration—Process for harvesting ESI from tapes for e-Discovery or because tapes are damaged, obsolete, or difficult to maintain, and storing harvested ESI on alternative media.

Task/Resource Schedule—A project management form used to define the timeline for tasks and people to complete deliverables. Also see *Deliverable*.

Temporary File—Files temporarily stored on a computer by Internet browsers and office applications to enable faster screen display. Forensic techniques may reveal computer usage through examination of temporary files.

Terabyte—See *Byte*.

Text Messaging—Sending/receiving short messages (160 characters or less) between mobile devices or computers.

Thread—Usually refers to a series of communications on a particular topic such as might take place with emails, bulletin boards, or messaging systems.

TIFF (Tagged Image File Format)—A widely used graphic file format for storing bit-mapped images with different compression formats and resolutions.

Transactional File System—Specialized file system enabling high volume transactions with fault tolerance, transaction roll back, and audit logging—typically used in financial systems.

Transcript Formats—Discovery and trial transcripts available electronically that can be searched, annotated, linked, and organized into brief reports in ALS Systems and in dedicated transcript management programs.

Transparency—The inherent feature of a process or system to be easily externally viewed or audited.

Trial Presentation—The display of evidence via computer display at a hearing rather than by way of multiple photocopies. Full-featured ALS Systems have built-in trial presentation features.

True Attachments—See *Attachments* and *Unitization.*

U

Unstructured ESI—Information not easily readable by machine or suitable to a database structure, such as email content, and audio or video files and unstructured text such as the body of an email or word processing document. Also see *Structured ESI*.

USB Drive—Small removable storage device that uses flash memory and connects via a USB port.

V

Validation—Various automated processes used to ensure the accuracy of scanned images and coded information, and to verify the accuracy of attachment ranges and dates.

Verbatim Coding—Extracting data from documents in a way that exactly matches the information as it appears in the documents.

Vertical Deduplication—A process through which duplicate documents or information are eliminated within a single custodial or production document set. Also see *Deduplication*.

Voice Mail—Recording in a file of analog or digital voice message.

VoIP (Voice over Internet Protocol)—Transmission of voice across an Internet connection, often with limited

attachments such as images and video.

W

WAN—Wide Area Network.

Web Repository—A Web Repository is part of an ALS System made available for users to perform required functions of document review via secure connection to the Internet, with no local software required other than a Web browser.

Web Server—Server specialized for transactions via the Internet.

Workflow—The automation of a function or process whereby ESI or tasks are passed from one user to another for action according to predefined rules.

WORM Discs—WORM (Write Once Read Many) discs are primarily used to archive information that must not be altered.

X

XML (Extensible Markup Language)—Specification for enabling users to define their own elements to facilitate sharing structured data across different information systems, particularly the Internet.

Y

Yottabyte—See *Byte.*

Z

Zettabyte—See *Byte.*

BIBLIOGRAPHY

BOOKS

BOB BECKER, RALPH KIMBALL, JOY MUNDY, MARGY ROSS & WARREN THORNTHWAITE, THE DATA WAREHOUSE LIFECYCLE TOOLKIT (2nd ed. New Jersey: John Wiley & Sons, Inc. 2008).

ADAM I. COHEN & DAVID J. LENDER, ELECTRONIC DISCOVERY: LAW AND PRACTICE (New York: Aspen Publishers 2007).

ADAM I. COHEN & EDWARD KALBAUGH, ESI HANDBOOK: SOURCES, TECHNOLOGY AND PRACTICE (Wolters Kluwer Publishers 2009).

ENCYCLOPEDIA OF TECHNOLOGY TERMS (Greg Wiegand, ed., Indiana: QUE Publishing 2002, Updated 2008). Internet: www.whatis.com

RONALD J. HEDGES, DISCOVERY OF ELECTRONICALLY STORED INFORMATION: SURVEYING THE LEGAL LANDSCAPE (BNA Books 2007).

SHARON D. NELSON, BRUCE A. OLSON & JOHN W. SIMEK, ELECTRONIC EVIDENCE AND DISCOVERY HANDBOOK: FORMS, CHECKLISTS AND GUIDELINES (Illinois: American Bar Association 2006).

W. CURTIS PRESTON, BACKUP & RECOVERY (California: O'Reilly Media 2007).

R. KELLY RANIER, JR. & EFRAIM TURBAN, INTRODUCTION TO INFORMATION SYSTEMS: SUPPORTING AND TRANSFORMING BUSINESS (2nd ed. New Jersey: John Wiley & Sons, Inc. 2008).

STEVEN A. WEISS & DAVID COALE, E-DISCOVERY (Illinois: American Bar Association 2007).

ARTICLES/PAPERS/REPORTS

Advisory Group to the New York State-Federal Judicial Council, *Harmonizing the Pre-Litigation Obligation to Preserve Electronically Stored Information in New York State and Federal Courts,* September 2010.

Association of the Bar of the City of New York: Report of Joint Committee on Electronic Discovery, *Explosion of Electronic Discovery in All Areas of Litigation Necessitates Changes in CPLR*, August 2009.

Jenifer A. L. Battle, *Saving ESI With 'Litigation Hold' Letters*, THE LEGAL INTELLIGENCER, July 13, 2007.

Jenifer A. L. Battle, *Saving ESI With 'Litigation Hold' Letters*, Law.com, July 13, 2007, *available at* http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1184231195691.

Steven C. Bennett, *Are E-Discovery Costs Recoverable By A Prevailing Party?* 20:3 ALBANY LAW J. OF SCI. & TECHNOL. 537-57 (2010).

Steven C. Bennett & David Cloud, *Coping with Metadata,* 61:2 MERCER L. REV. 471-89 (2010).

Steven C. Bennett, *Ethical Dimensions Of The New Federal Rules On E-Discovery*, 16:12 AM. LAW CORP. COUNSEL Supp. 16-18 (2009).

Marla S. Bergman & Steven C. Bennett, *Managing E-Discovery Costs*, PRACTICAL LITIGATOR 57-63 (July 2009).

Mark A. Berman, *Case Law Remains Unclear as to Who Pays for What,* NEW YORK LAW JOURNAL, Jan. 4, 2011.

Mark A. Berman, *Overbroad Demands and Improper Denials*, NEW YORK LAW JOURNAL, March 1, 2011.

Mark A. Berman, Anne D. Taback, & Aaron E. Zerykier, *Now That Everything Is Collected, How to Produce It?* NEW YORK LAW JOURNAL, March 21, 2011.

Mark A. Berman, *Recent Rulings Founded on Spoliation of ESI,* NEW YORK LAW JOURNAL, May 3, 2011.

H. Christopher Boehning & Daniel J. Toal, *Cost-Shifting and Accessible Data in EDD*, NEW YORK LAW

JOURNAL, June 28, 2007.

John Chivvas, *Discovering E-Discovery*, ROUGH NOTES MAGAZINE, October 2006.

John Chivvas, *The Evolution of Document Management*, ROUGH NOTES MAGAZINE, September 2007.

Adam I. Cohen, *How New Technology Reduces the True Cost of e-Discovery,* LAW JOURNAL NEWSLETTER, Volume 25, Number 2, May 2007.

Adam I. Cohen, *Understanding e-Discovery Risks*, FTI Consulting, Inc., 2007.

Patrick M. Connors, *Which Party Pays the Costs of Document Disclosure?* 29 PACE L.R. 441 (2008-09).

Michael Dolan, & Dario Olivas, *Legal Process Outsourcing of First Level Document Review,* TUSKER GROUP, *available at* http://www.sourcingmag.com/content/c060918a.asp.

Meg Fletcher, *E-Discovery Falls Hardest On Insurance Industry*, BUSINESS INSURANCE EUROPE, May 2007.

Brian Fonseca, *E-discovery Rules Still Causing IT Headaches,* COMPUTERWORLD, Jan. 7, 2008.

Ann G. Fort, *Rising Costs of E-Discovery Requirements Impacting Litigants,* FULTON COUNTY DAILY REPORT March 20, 2007.

Lynn Haber, *E-Discovery: Reducing the Cost of Review,* SEMANTEC CORPORATION, Feb. 14, 2007, *available at* http://www.devx.com/symantec/Article/33749.

Robert L. Haig, *Making the Case for Change*, ABA JOURNAL, April 2008.

Conrad J. Jacoby, *E-Discovery Update: Recognizing Hidden Logistical Bottlenecks in E-Discovery, at* LLRX.com (April 24, 2007).

Stanley P. Jaskiewicz, *E-Lawyering Requires Rethinking Technology and Law, Internet Law & Strategy,* THE ESTRIN REPORT, March 16, 2007, *available at* http://estrinlegaled.typepad.com/my_weblog/2007/03/elawyering_requ.html.

Stanley P. Jaskiewicz, *Follow the Mail: Don't Let Your Employees' Multiple E-Mail Boxes Become An Electronic Nightmare*, E-DISCOVERY LAW & STRATEGY, July 10, 2007, *available at* http://infogovernance.blogspot.com/2007/07/follow-mail-legal-technology.html.

Joint E-Discovery Subcommittee of The Association of The Bar of the City of New York, MANUAL FOR STATE TRIAL COURTS REGARDING ELECTRONIC DISCOVERY COST ALLOCATION, Spring 2009.

Preggy Bresnick Kendler, ed., *Virtual Roundtable: The Age of e-Discovery,* INSURANCE□+□TECHNOLOGY, March 2007, CMP Media.

Elizabeth Millard, *IM and Texting Are Here To Stay*, PROCESSOR MAGAZINE, Oct. 12, 2007.

Vivian Tero, *State of Play: Litigation Readiness of the Corporate IT Infrastructure*, IDC, May 8, 2008.

The New York State Unified Court System, *A Report to the Chief Judge and Chief Administrative Judge, Electronic Discovery in the New York State Courts*, February 2010.

Alex Vorro, *e-Discovery: A Way To Paperless Organization*, INSURANCE NETWORKING NEWS AND SOURCEMEDIA, INC. , April 1, 2008.

Kenneth J. Withers, *Annotated Case Law on Electronic Discovery*, FEDERAL JUDICIAL CENTER, July 5, 2006, *available at* www.fjc.gov/public/pdf.nsf/lookup/ElecDi09.pdf.

INTERNET REFERENCES

American Bar Association (Resources for Lawyers), *at* http://www.abanet.org/.

CGOC (Compliance Governance Oversight Council), *at* http://www.cgocouncil.com/about/index.html.

EDD Blog Online (Information source and discussion forum for e-Discovery issues) , *at* http://www.eddblogonline.com/.

e-Discovery Law, *at* http://www.e-Discoverylaw.com.

EDRM (E-Discovery Reference Model and forum for legal and e-Discovery practitioners), *at* http://www.edrm.net.

Federal Judicial Center (Materials on Electronic Discovery), *at* http://www.fjc.gov/public/home.nsf/autoframe?openform&url_l=/public/home.nsf/inavgeneral?openpage&url_r=/public/home.nsf/pages/196.

FindLaw for Legal Professionals (e-Discovery articles), *at* http://technology.findlaw.com/.

International Journal of Digital Evidence (Discussion forum in the field of digital evidence hosted by Utica College), *at* http://www.utica.edu/academic/institutes/ecii/ijde/index.cfm.

IT Management Resource Centers (Information and discussion forum for variety of IT functional areas and issues), *at* http://www.itmanagement.com/.

Law.Com, Legal Technology (e-Discovery articles and blogs) http://www.law.com/jsp/legaltechnology/edd.jsp.

Litigation Support Vendors Association (not-for-profit forum for major software companies covering e-Discovery) http://www.lsva.com/pn/.

LLRX.com (Law and technology Web journal for legal community) http://www.llrx.com/.

NIST (U.S. National Institute of Standards and Technology) http://www.nist.gov.

Sedona Conference (Forum for legal and e-discovery practitioners) http://www.thesedonaconference.org/.