

I N S I D E T H E M I N D S

Electronic Records Management and e-Discovery

*Leading Lawyers on Navigating Recent Trends,
Understanding Rules and Regulations, and
Implementing an e-Discovery Strategy*



ASPATORE

©2010 Thomson Reuters/Aspatore

All rights reserved. Printed in the United States of America.

No part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, except as permitted under Sections 107 or 108 of the U.S. Copyright Act, without prior written permission of the publisher. This book is printed on acid free paper.

Material in this book is for educational purposes only. This book is sold with the understanding that neither any of the authors nor the publisher is engaged in rendering legal, accounting, investment, or any other professional service. Neither the publisher nor the authors assume any liability for any errors or omissions or for how this book or its contents are used or interpreted or for any consequences resulting directly or indirectly from the use of this book. For legal advice or any other, please consult your personal lawyer or the appropriate professional.

The views expressed by the individuals in this book (or the individuals on the cover) do not necessarily reflect the views shared by the companies they are employed by (or the companies mentioned in this book). The employment status and affiliations of authors with the companies referenced are subject to change.

Aspatore books may be purchased for educational, business, or sales promotional use. For information, please email West.customer.service@thomson.com.

For corrections, updates, comments or any other inquiries please email TLR.AspatoreEditorial@thomson.com.

First Printing, 2010

10 9 8 7 6 5 4 3 2 1

If you are interested in purchasing the book this chapter was originally included in, please visit www.west.thomson.com.

From Preservation to
Production: The Dos and
Don'ts of e-Discovery
in Litigation

Michael C. Lasky and Marc J. Rachman

Partners

Davis & Gilbert LLP



ASPATORE

Regulations Governing Electronic Records and e-Discovery

For cases in federal court, the Federal Rules of Civil Procedure contain specific rules governing electronic records and discovery. For cases in state court, some state courts follow the rules set forth in the Federal Rules of Civil Procedure, but many do not, and either have their own rules governing electronic records and discovery or rely on court decisions on the subject.

Given the variations from state to state and between state procedure and the Federal Rules of Civil Procedure, we will focus on the Federal Rules of Civil Procedure in this chapter.

The Federal Rules of Civil Procedure

The Federal Rules of Civil Procedure were amended in 2006 to address e-discovery more specifically. The following new/modified rules concern electronically stored information (ESI) and e-discovery:

- Rule 16 – Concerning pretrial conferences and amending subsection 16(b) to address the handling of electronically stored information early in the litigation if such discovery is expected to occur.
- Rule 26 – General provisions governing discovery; subsection (f) now requires the parties to discuss discovery of ESI; subsection (b)(5)(B) now provides a mechanism by which parties may “claw back” inadvertently produced privileged information.
- Rule 33 – Concerning interrogatories, amended to parallel Rule 34(a) to address ESI.
- Rule 34 – Concerning requests for documents, amended to add “electronically stored information” to the types of documents/information a party may request; also added subsection (b)(1)(C) to allow parties to specify the form(s) in which ESI is to be produced; subsection (b)(2)(D) allowing a responding party to object to a requested form of production; and subsection (b)(2)(E)(ii) requiring a party to produce ESI in the form(s) in which it is ordinarily maintained or in a reasonably usable form.

- Rule 37 – Concerning sanctions for failure to make disclosures or cooperate in discovery; includes what has been popularly regarded as a “safe harbor” limit on sanctions under Rule 37 for the loss of electronically stored information as a result of the routine operation of computer systems. ¹
- Rule 45 – Governing non-parties’ obligations in responding to subpoenas for documents and corresponding to changes in Rules 26, 33, 37.

Table 1

Federal Rules of Evidence Concerning ESI

<u>Federal Rule</u>	<u>Description</u>
Rule 16 (b)(3)(B)(iii)	Pretrial Scheduling Order may provide for disclosure or discovery of ESI
Rule 26(b)(5)(B)	Party may assert claim of privilege or work product over information produced in discovery, triggering the receiving party’s duty to return, sequester or destroy the information and refrain from use or disclosure until the claim is resolved.
Rule 26(f)(3)(c)	Parties must meet and confer and include issues about disclosure or discovery of ESI in their discovery plan.
Rule 33(d)	Response to interrogatories may be made by specifying records, including specifically ESI, that must be reviewed and allowing the interrogating party to inspect/audit/copy/ summarize the records.
Rule 34(b)(1)(C)	Request for production of documents may specify the form(s) in which ESI is to be produced.
Rule 34(B)(2)(D)	Party may object to request for production of

¹ The Hon. Lee H. Rosenthal, Chair of the Committee that drafted the 2006 amendments to the Federal Rules, does not agree that Rule 37 is a true “safe harbor,” as the limit on sanctions is preceded by the language “absent exceptional circumstances.” “Electronic Discovery: Views from the Judges,” 76 Fordham L. Rev. 1 (October 2007), p. 10.

	ESI or requested form; party must state form(s) it intends to use.
Rule 34 (b)(2)(E)(ii)	If request for production of ESI does not specify form, a party must produce it in a form which is ordinarily maintained or in a reasonably useable form.
Rule 34 (b)(2)(E)(iii)	ESI only needs to be produced in one form.
Rule 37(e)	Court may not impose sanctions for failing to provide ESI lost as a result of a routine, good faith operation of an electronic information system absent exceptional circumstances.
Rule 45(d)(1)	Setting forth rules re ESI in context of non-party subpoenas, and providing that ESI from sources that are not reasonably accessible need not be produced.

Federal Rules of Evidence - Rule 502

Rule 502 of the Federal Rules of Evidence was added in 2008 to address, at least in part, the privilege review problem. It is also addressed, in part, in Rule 26(b)(5)(B).

The issue relates to the inadvertent disclosure of privileged materials, which in certain circumstances can lead to a waiver of the attorney-client or work product privilege. Potentially, such a waiver could lead to a subject matter privilege waiver, opening the door to discovery of other related privileged communications. Expensive and time-consuming privilege reviews are therefore necessary to minimize or eliminate the risk of a privilege waiver.

In order to address the friction between requiring voluminous productions of electronic records and the potential for inadvertent privilege waiver, Federal Rule of Evidence 502 was enacted. It provides that when inadvertent disclosure of privileged or work product material occurs in a federal proceeding or is made to a federal office or agency, the disclosure does not operate as a waiver of privilege in any proceeding

(federal or state) provided that certain criteria are met. Specifically, the disclosure must be inadvertent and the privilege holder must take reasonable steps to prevent disclosure and promptly rectify the error. It also limits the effect of a privilege waiver resulting from inadvertent disclosure of privileged material in a state proceeding in a subsequent federal proceeding. Rule 502, together with the amendments to Rule 26, do not eliminate the need for a privilege review—many litigants are justifiably concerned that they will not be able to “unring the bell” if privileged information is disclosed—but they do provide parties producing voluminous information with some protection for errors in review or processing.

Need for Additional Regulation

One of the major e-discovery issues that demands further attention, though not necessarily further regulation, is proportionality. The time/money cost of exhaustively gathering, searching, and producing ESI can dwarf the amount in controversy in many cases. Additionally, ESI means that there is more metadata—“information about information”—available than ever before. A requesting party receiving, in a document production, a copy of a letter sent by U.S. mail will not have access to as much information about the letter as a requesting party who receives the Word version of the same letter in electronic format attached to an e-mail—e.g., time sent/received, creation and editing dates, tracked changes, etc. Also, with ESI, there are likely to be more copies or versions of a document than with hard copies. People tend to treat e-mail as a means of conversation, and given the ease with which an e-mail can be sent to many people at once, a company may find itself with dozens or even hundreds of copies of the same e-mail, all of which potentially could be responsive to a document request.

The costs and burdens of e-discovery are, therefore, factors that may be driving a perceived need for additional regulation.² However, it is not

² The costs start adding up even before documents are requested or collected for production. As discussed further below, a party who reasonably anticipates litigation has a duty to preserve all potentially relevant information. This can significantly add to a company’s ESI management and storage costs. The fear of spoliation allegations and

clear to these authors whether additional regulations would help to alleviate the burden of e-discovery on parties. Absent an outright ban on requesting information on backup tapes, or a legislated limit on the number of custodians whose e-mails would have to be searched in response to a request, neither of which are practical solutions, it is hard to see how additional rules will help parties cut down on the costs of preservation and production.

The principle of proportionality underlies the rules we already have. Assessing how much burden a party should bear in discovery, and how big a burden needs to be before it is considered “undue,” necessarily varies from case to case. What is excessive in a \$25,000 dispute may be more than reasonable in a multi-million dollar dispute. Moreover, there is flexibility in the current regulations that provide protections to a producing party—e.g., the broad term ESI; the fact that the definition of “inaccessible” data is subject to interpretation in every case; the ability of the courts to fashion remedies (e.g., cost-shifting) where discovery costs and burden threaten to spin out of control, etc.

Additionally, there is always the possibility that technological advances will make any more specific, bright-line rules obsolete. For example, in 2003 and 2004, when the seminal *Zubulake* decisions concerning e-discovery were issued, *Zubulake v. UBS Warburg LLC*, 216 F.R.D. 280 (S.D.N.Y. 2003); *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003); *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212 (S.D.N.Y. 2003); *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422 (S.D.N.Y. 2003), backup tapes were generally considered inaccessible, and in most cases, far too expensive to restore and search. Since then, litigants have generally assumed that a request for backup tapes will lead to an arduous and expensive restoration project requiring cost-shifting. Yet, technological advances have allowed companies to engage in a more dynamic data backup process in many companies, and backup records are no longer necessarily offline, kept on inaccessible tapes. This is one of the reasons that the term “backup tape” is not found in the 2006 amendments to the Federal Rules.³

sanctions for failure to preserve ESI may even drive parties to preserve a far greater amount of ESI at greater cost than is necessary.

³ See “Electronic Discovery: Views from the Bench,” 76 *Fordham L. Rev.* 1 (Oct. 2007), including commentary by the Hon. Lee Rosenthal, United States District Court Judge for

Certain judges—notably the Hon. Shira Scheindlin of the United States District Court for the Southern District of New York (who decided *Zubulake*) and the Hon. Lee Rosenthal of the United States District Court for the Southern District of Texas (who chaired the committee charged with drafting amendments to the Federal Rules of Civil Procedure)—have taken a leading role in providing clarity to litigants concerning the scope of their electronic discovery obligations, including the extent of their obligation to preserve documents once they reasonably anticipate litigation. As eager as litigants are for easy-to-follow rules of do’s and don’ts for preservation and production, these leading jurists have expressed their reluctance to set absolute standards.

In fact, Judge Scheindlin qualified her recent decision concerning sanctions for e-discovery failures in *Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec. LLC*, 2010 WL 184312 (Jan. 1, 2010). In an opinion related to e-discovery in this case, she stated: “I stress that at the end of the day the judgment call of whether to award sanctions [for discovery failures] is inherently subjective...while it would be helpful to develop a list of relevant criteria a court should review in evaluating discovery conduct, *these inquiries are inherently fact intensive and must be reviewed case by case.*” *Id.* At *7. (Emphasis added.) Judge Scheindlin then went on to list discovery failures that would support a finding of gross negligence when a duty to preserve documents has arisen. This guidance is certainly helpful and should be taken into account when faced with a document preservation obligation. Judge Scheindlin listed the following failures in support of her finding that certain plaintiffs had engaged in gross negligence with respect to their preservation duties:

- Failure to issue a written litigation hold
- Failure to identify key players and ensure their electronic and paper records are preserved

the Southern District of Texas in Houston, who also served on and became chair of the Judicial Conference Advisory Committee for Rules of Civil Procedure, which promulgated the 2006 changes to the Rules. Judge Rosenthal states that the term “backup tapes” was not included in the final version of the amended rules. As she explained, “Backup tapes, which had been these big, ungainly things that were not indexed or searchable, now are smaller and often searchable.” *Id.*, p. 7.

- Failure to cease deletion of e-mail in the face of a preservation obligation
- Failure to preserve former employee records that are in a party's possession, custody, or control
- Failure to preserve backup tapes when they are the sole source of relevant information or relate to key players

As useful as this information is, there is a risk that parties may interpret them as new “bright-line” rules, compliance with which means safety from sanctions, and violation of which always leads to dire consequences. This, however, is not how the decision should be read. A plaintiff's idea of the key players may be different from a defendant's idea. Moreover, what should or should not be a sanctionable e-discovery failure often depends on the facts of a given case. For example, in *Rimkus Consulting Group Inc. v. Cammarata*, 2010 WL 645253 (S.D. Tex., Feb. 19, 2010) decided February 19, 2010 by the Hon. Lee H. Rosenthal, the Court held that certain sanctions were not appropriate for anything short of intentional misconduct—in contrast to *Pension Committee*, in which severe sanctions (an adverse jury instruction) were ordered where the parties were found to have been grossly negligent. Judge Rosenthal noted that, on the *Rimkus* record, there was “conflicting evidence about the reasons the defendants deleted the e-mails and attachments; evidence that some of the deleted e-mails and attachments were favorable to defendants, and an extensive amount of other evidence for the plaintiff to use.”

These two cases illustrate the problem with boiling the sophisticated, lengthy reasoning in these decisions down to a list of “do's” and “don'ts”—such a list may provide false comfort, or encourage pursuit of sanctions where no real harm occurred. The real issue is not always whether there was or was not a particular e-discovery failure that can be checked off a list, but whether it made any real difference in the case, and whether the producing party took reasonable steps in the face of the request(s) seeking the production of ESI.

Key Players in Changing the e-Discovery Rules

The key e-discovery-related amendments to the Federal Rules of Civil Procedure were the result of work by the Standing Committee on the Rules of

Practice and Procedure of the Judicial Conference and the Civil Rules Advisory Committee. Additionally, e-discovery rules and regulations are evolving in part because of the challenges that parties face responding to discovery.

Some judges are also deeply involved in this area. The Hon. Shira Scheindlin and the Hon. Lee Rosenthal, whose recent e-discovery decisions are discussed briefly above, are recognized as leading jurists in e-discovery. The Sedona Conference has also done considerable important work in this field—work on which many judges have relied in analyzing parties’ efforts to preserve and produce responsive documents. The Sedona Conference is a nonprofit organization, whose mission is “to allow leading jurists, lawyers, experts, academics, and others, at the cutting edge of issues in the area of antitrust law, complex litigation, and intellectual property rights, to come together—in conferences and mini-think tanks (Working Groups).” www.sedonaconference.org. Principles and commentaries issued by the Sedona Conference are frequently cited by the courts. See, for example, the *Zubulake* decisions by Judge Scheindlin. Some of the key Sedona Conference publications in this area are:

- Commentary on Inactive Information Sources (July, 2009)
- Commentary on Preservation, Management and Identification of Sources of Information that are Not Reasonably Accessible (August, 2008)
- Commentary on Non-Party Production and Rule 45 Subpoenas (April, 2008)
- Commentary on Legal Holds (August, 2007)

All of these may be found online at:

http://www.thesedonaconference.org/content/miscFiles/publications_html?grp=wgs110

Intent of Legal Standards in e-Discovery

The discovery standards in the Federal Rules of Civil Procedure show an intent to balance litigants’ needs for full disclosure of all information relevant to any claim or defense with the need to protect responding parties from disproportionate burden and expense.

The basic principle governing all discovery, including e-discovery, is found in Rule 26(b)(1):

Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any non-privileged matter that is relevant to any party's claim or defense—including the existence, description, nature, custody, condition and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter... Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to discovery of admissible evidence.

The same limitations apply in the e-discovery sphere as with any other discovery, and proportionality is the key consideration. Indeed, Rule 26(b)(2)(C) requires courts to limit the frequency or extent of discovery if it is cumulative, duplicative, can be obtained from another source that is more convenient, less burdensome, or less expensive, or if the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues.

Balancing the need for relevant information with the burden of obtaining that information also underlies the amendments to Rule 16 and 26(f), as parties are now required to meet and confer early in a litigation concerning any issues about disclosure or discovery of ESI, including the form or forms in which it should be produced.

e-Discovery Strategies

The below discussion is predicated on the assumption that a party's goal is to obtain proportionate, thorough discovery to flesh out all the real issues in a dispute, avoid needlessly costly pitfalls, and get as efficiently as possible to settlement, summary judgment, or trial. As the recent *Pension Committee* and *Rimkus* decisions show, however, serious potential traps for litigants lie in the preservation of documents, before discovery even begins in earnest. Thus, this discussion focuses particularly on preservation issues.

Components of an E-Discovery Strategy

The components of an e-discovery strategy can be described in a few simple steps, but of course, the devil is in the details:

1. Know what information you have that may be relevant to any party's claims or defenses.
2. Preserve it in a timely manner,⁴ and diligently follow up.
3. Identify the information you need to support your claims and defenses.
4. If you have it, produce it. If you do not, go and get it through discovery.

Many an expensive and painful discovery dispute has arisen because a party failed to identify relevant information before it was lost or migrated to an inaccessible (or only expensively accessible) location. If e-mails are currently accessible on a company's server, a snapshot of relevant accounts should be taken now rather than risking loss of the e-mails, or having to retrieve them from backup tapes down the road.⁵ Moreover, understanding the documents you already have is necessary to formulate requests for documents from parties and/or to determine if documents will need to be obtained from third parties.

Thus, the first step—knowing what you have—is critical to designing a proper document preservation strategy and the cornerstone for building an overall discovery strategy.⁶

⁴ As noted above, the duty to preserve evidence is triggered by either the filing of a lawsuit or even earlier if a party has notice that future litigation is likely. *See, e.g., Cache La Poudre Feeds LLC v. Land O' Lakes Inc.* 244 F.R.D. 614 (D. Colorado, 2007) (discussing when the preservation duty arose, and concluding that, while the duty may arise when a party has notice that future litigation is likely, "something more than an equivocal statement of discontent" is required).

⁵ A party can lose a cost-shifting argument, however, if an expensive restoration/retrieval process would not have been needed if the party had properly preserved accessible documents once the duty to preserve arose. *See, e.g., Peskoff v. Faber*, 251 F.R.D. 59 (D. Columbia, 2008) (because defendant failed to preserve e-mails and allowed auto-deletion process to continue after duty to preserve arose, costs of expensive forensic examination would not be shifted to the requesting party); *Quinby v. WestLB AG*, 245 FRD 94 (SDNY, 2006) (party not entitled to shift the costs of restoring and searching data that it converted into an inaccessible format at a time when it should have anticipated litigation).

⁶ Attached as an appendix is a checklist for attorneys guiding their clients' document preservation efforts

A good understanding of the sources of ESI, and the methods and costs associated with retrieval of ESI, are key to formulating objections to discovery requests or opposing motions to compel production. Judges are not likely to grant a protective order or deny a motion to compel production of ESI based on a party's assertion of cost and burden alone. However, a requesting party may be required to pay costs of retrieval/processing (cost-shifting), or discovery may be denied if a party can make a strong showing that the burden is disproportionate to the claims in the case.

The second step of preservation is critical to avoid expensive and potentially disastrous distractions from the ultimate dispute in a given case. Parties may have legitimate objections (relevance, privilege, burden, expense, etc.) to requests for discovery. A party that has properly preserved documents can fight a motion to compel production of ESI to which it has objected. If it loses, it can produce the ESI as ordered by the court and live to fight another day. However, if the ESI has been destroyed in the meantime—intentionally, negligently, or otherwise—the failure to preserve documents can potentially be a case killer.

Notably, failure to preserve documents led to sanctions in both the *Pension Committee* and *Rimkus* cases discussed above. In *Pension Committee*, 2010 WL 184312, thirteen plaintiffs were found to have been at least negligent in their efforts to meet their discovery obligations. All were required to pay monetary sanctions, and the Court determined that it would issue an adverse inference instruction to the jury for the six worst offenders. The jury would then be permitted, but not required, to find that the lost or destroyed evidence would have been favorable to the defendants. Judge Scheindlin noted that, had she found the plaintiffs deliberately destroyed documents, even harsher sanctions could have ensued, from an instruction to the jury that it *must* assume the lost or destroyed documents were relevant and favorable to the defendant, to dismissal of the plaintiffs' case in its entirety. In *Rimkus*, 2010 WL 645253 *32, Judge Rosenthal noted in her analysis that, while some loss of documents had occurred due to the defendants' deletion of them, the damage was "far from irreparable" because the defendants had produced some of the documents, and *Rimkus* had been able to obtain deleted records from other sources. *Id.* At *34. Thus, Judge Rosenthal concluded that the most extreme sanction—default judgment or dismissal—was not appropriate, but due to the defendants' intentional destruction of documents after the duty to preserve had arisen, a form of adverse inference instruction would be given. *Id.*

For the third and fourth steps—identifying information you need and producing it or seeking discovery to get it—a consideration must be given to metadata. In some cases, metadata can be of minimal importance. In others, it can be critical. If there could be an issue as to when an e-mail was sent or received, if it was read, whether a document was copied or modified, and if so, how and when, who wrote and commented on a document, when an invoice was transmitted, etc., then serious consideration should be given to demanding that documents be produced or to producing documents in native file format.⁷ If producing electronically-stored documents that are in part privileged, or contain irrelevant information concerning other products or clients, it may be wiser to produce them in searchable TIFF or PDF form⁸ with redactions, providing appropriate metadata fields, in a discovery database such as Concordance or Summation. Below is a table showing examples of the various different file types in which ESI may be stored.

⁷ Native file format means the default file format a computer program uses to store data on a drive or disk. For example, a Word document is saved to a drive or disk as a Word file (with a .doc file name extension) and producing it in native file format means producing it as a Word file, rather than as a printed hard copy document, pdf, or other formatted file. The recipient can then open the document on his or her computer using Word. Depending on the e-mail program, e-mails may be saved, with their attachments and data concerning their transmission, in a compressed file. For Microsoft Outlook, this is usually a .pst file. Again, the recipient of a native file format production of e-mails in .pst files can load those documents onto his/her computer, and view them in the Microsoft Outlook program.

⁸ TIFF (Tagged Image File Format) and PDF (Portable Document Format) files are types of “petrified” electronic documents. One way to think of them is the equivalent of a photocopy, except viewable on a computer screen. These types of files may be made so that they are searchable, or so that a user can sort them by metadata fields such as sender, recipient, date sent/received, etc. A Word document or e-mail produced as a TIFF or PDF file may be scrubbed of metadata, or redacted. The advantage of TIFF and PDF files is that they cannot be edited, they are viewable on most computers even if the recipient does not have the same proprietary software (such as Microsoft Word, Photoshop, or QuickBooks) and the recipient will not be able to see any redacted material; however, since they can be scrubbed of all metadata or produced with selected metadata only, and sorting/organizing them may require specific case management software, a requesting party may have a preference for native file format where possible.

Table 2

Example File Types

<u>File Extension</u>	<u>Description</u>
Archives	
.7z	Archived File
.zip	Archived File
.rar	Archived File
Databases	
.dat	DOS Basic
.mdb	Microsoft Access
.nsf	Lotus Notes database
Personal Information Manager	
.msg	Microsoft Outlook manager
.pst	Microsoft Outlook email communication
.mbox	Apple Outlook manager
Documents	
.csv	Ascii text encoded as comma separated values
.doc	Microsoft Word
.docx	Microsoft Office Word 2007 for Windows/2008 for Mac
.html	Hypertext Markup Language
.pdf	Portable Document Format
.rtf	Rich Text Format
.txt	Wordperfect document
.wpd	Microsoft Works document
.wps	Microsoft PowerPoint Presentation
.ppt	Office Open XML Presentation
.pptx	Office Open XML Presentation

.xls	Microsoft Excel spreadsheet
.xlsx	Office Open XML worksheet sheet
.123	Lotus Notes 1-2-3
Graphics	
.bmp	Microsoft Windows bitmap formatted image
.jpeg	Image format widely used to display photographic images
.gif	Graphics Interchange Format
.png	Portable Network Graphic
.psd	Adobe photoshop drawing
.tiff	Tagg Image File Format
Sound, Music, Video	
.wav	Sound/Music file
.wma	Sound/Music file
.mp3	Sound/Music file
.avi	Sound/Music file
.flv	Video file
.mov	Video file
.mpeg	Video file
.wmv	Video file
.swf	Video file

In all cases, the revised Federal Rules of Civil Procedure mandate that the parties confer regarding the method of production for ESI. In *Covad Communications Co. v. Revonet Inc.*, 254 F.R.D. 147 (D. Columbia, 2008), a dispute concerning the alleged conversion and misappropriation of trade secrets, the parties found themselves in a dispute over the form of production of e-mails. The defendant had already produced the e-mails at issue in hard copy form, and the plaintiff demanded they be produced in native form. In *Covad*, the initial hard copy production had been made before the revised Federal Rules took effect, but the court noted that the

defendant was “playing with fire” by producing the e-mails only in hard copy form in light of *Zubulake* and other e-discovery decisions. Ultimately, the parties were required to split the costs of having a paralegal remove privileged e-mails from the native file format collection of e-mails. The court said: “Since both parties went through the same stop sign, it appears to me that they both should pay for the crash. . . . I would hope that my decision will have a didactic purpose. This whole controversy could have been eliminated had Covad asked for the data in native format in the first place or had Revonet asked Covad in what format it wanted the data before it presumed that it was not native.” The court’s decision and order illustrates not only the wisdom of conferring regarding the method of production of ESI, but also the courts’ impatience with avoidable discovery disputes on the issue.

When e-Discovery is Critical to the Case Being Litigated

There are few cases anymore in which e-discovery is not a significant part of the discovery process, if not a critical one. Below are listed different types of cases and situations that may arise in litigation, and the ways in which e-discovery can be a critical part of discovery in them.

Employment Discrimination

E-discovery often proves to be a critical part of an employment discrimination case. Using the example of where a company is accused of discrimination by a former employee, if the offending supervisors’ e-mails contain discriminatory comments about the employee or others in his or her protected class, it could be “game over” for the employer. Or, conversely, if the employee’s e-mail account or browser history at work contains evidence that he or she spent all day on non-work related projects, or forwarded the employer’s confidential and proprietary information to a competitor, an employer’s legitimate business reasons for terminating that employee may go from plausible to indisputable.

Indeed, *Zubulake v. UBS Warburg*, 217 F.R.D. 309 (S.D.N.Y. 2003), which provided the forum for Judge Scheindlin’s much-cited e-discovery opinions, was a gender discrimination lawsuit. The plaintiff had requested that the defendant produce all documents concerning any communications by or

between UBS employees concerning the plaintiff. After UBS produced documents, the plaintiff knew that UBS had not produced all such communications because she herself was in possession of more such documents than UBS had produced. The court ordered restoration of UBS's archival media and searches and deferred a determination on cost-shifting until after this was completed. After the restoration effort, during which it was revealed that some e-mails and archives had been destroyed, Judge Scheindlin found that UBS was in violation of its document preservation duties. *Zubulake v. UBS Warburg*, 220 F.R.D. 212 (S.D.N.Y. 2003). The Court did not order an adverse inference instruction, but did order the defendant to bear the plaintiff's costs to re-depose certain witnesses to inquire into destruction of evidence and concerning newly discovered e-mails.⁹ After this was done, the plaintiff moved again for sanctions, which were granted, as the court found that UBS had failed to locate, preserve, and timely produce information and sanctioned UBS for over \$200,000 in costs. *Zubulake v. UBS Warburg*, 229 F.R.D. 422 (S.D.N.Y. 2004).¹⁰

Another example is *Jackson v. Planco*, 660 F. Supp. 2d 562 (E.D. Pa. 2009), which was a disability discrimination and retaliation case. In *Jackson*, the defendant employer moved for summary judgment and won. ESI played a critical role as the employer had evidence of the employee's Web browsing history, showing that the employee violated its Internet policies by viewing gun Web sites at the office.

⁹ Although the Court held that the costs for searches and retrieval of inaccessible ESI—*i.e.*, backup tapes—should usually be borne by the requesting party, given UBS's conduct, UBS had to bear three-quarters of the \$166,000 estimated costs to restore backup tapes, and all of the estimated \$108,000 costs to review documents on those tapes. *Zubulake*, 216 FRD 280 (S.D.N.Y. 2003).

¹⁰ The sanctions that were awarded included: (1) paying for re-deposition of relevant UBS personnel and other witnesses concerning new materials produced from backup tapes; (2) paying the costs of restoration and production of relevant documents from backup tapes; (3) an adverse inference instruction to the jury; and (4) paying the plaintiff's reasonable costs and attorney's fees for the sanctions motions. Additionally, the Court noted that UBS also had a "self-executing sanction" because the newly discovered e-mails seemed to contradict testimony of a UBS employee who had not had the benefit of reviewing these e-mails before his first deposition, and the plaintiff would be allowed, of course, to use that testimony at trial. *Id.*, 437, 439-440.

Restrictive Covenants

Another type of case where e-discovery can be critical is one involving claims relating to an employee's restrictive covenants. For example, *Rimkus*, 2010 WL 645253 (discussed above), involved restrictive covenants. The ESI at issue concerned former employees discussing leaving Rimkus to start a new, competing company, and taking/using Rimkus' confidential information to do so. It is not hard to imagine how an e-mail trail or metadata showing when particular documents were copied or accessed by former employees accused of competing unfairly with their former employer or violating their restrictive covenants could affect the outcome of a case.

Misappropriation of Trade Secrets

ESI can be used to show that trade secrets were appropriately protected, or to show that they had been shared and used in a manner that destroys their trade secret protection. For example, in *Lockheed Martin Corp. v. L-3 Communications Integrated Sys.*, 2010 WL 1891779 (N.D. Ga. 2010), the court tossed out a \$37.3 million trade secrets verdict for Lockheed Martin Corp. and ordered a new trial after finding that Lockheed had failed to turn over relevant e-mails concerning use of its purported trade secrets by another company without compensation to Lockheed. The court held that the defendant L-3 had been deprived of its opportunity to make the argument to the jury that the trade secret status of the proprietary information at issue had terminated when Lockheed allowed the other company to use it without compensation. The Court held that a terminating sanction was not appropriate because the harm to L-3 could be fixed by a new trial.

Copyright Infringement and Other Intellectual Property Matters

ESI can also prove critical in copyright infringement cases. For example, in *Columbia Pictures, Inc. v. Bunnell*, 2007 WL 4877701 (C.D. Cal., Dec. 13, 2007), a copyright infringement case, the court granted a default judgment due to spoliation of electronic evidence. This case concerned the defendants' alleged participation in illegal downloading and file sharing of copyrighted works (movies) produced by the plaintiffs. ESI was

critical: the plaintiffs needed full IP addresses to determine the full extent of the infringement and whether the defendants had actually infringed themselves. The defendants denied maintaining those records, but forum postings between moderators of the defendants' Web site referred to full IP addresses. The plaintiffs were able to show that the defendants "engaged in widespread and systematic efforts to destroy evidence" and "provided false testimony under oath in an effort to hide evidence of such destruction." After analyzing lesser sanctions such as exclusion of evidence or an adverse jury instruction, the Court found that the circumstances of the case were "sufficiently extraordinary" to merit the sanction of default judgment, as "lesser sanctions would not be adequate to punish the defendants for the wrongful conduct and ameliorate the prejudice and harm to the plaintiffs."

In *Capitol Records, Inc. v. MP3Tunes, LLC*, 261 F.R.D. 44 (S.D.N.Y. 2009), the parties hotly contested a number of e-discovery issues. Defendant MP3Tunes operated Web sites providing users with access to third party Web sites from which they could stream and listen to music and "sideload" music to a permanent "locker" assigned to them at www.MP3tunes.com. ESI was key to this dispute. The parties disagreed on the keyword search terms to use in MP3Tunes' e-mails. Ultimately, MP3Tunes was ordered to search for thirty different keywords in the e-mails of both senior and lower-level employees. MP3Tunes also sought to compel production of e-mails from plaintiffs, who argued that the e-mails were inaccessible. The court denied MP3Tunes' request, stating: "The day undoubtedly will come when burden arguments based on a large organization's lack of internal e-discovery software will be received about as well as the contention that a party should be spared from retrieving paper documents because it had filed them sequentially, but in no apparent groupings, in an effort to avoid the added expense of file folders or indices." However, the court still found the requested e-mails to be inaccessible, and limited what the plaintiffs would be required to search and produce.

ESI can also be critical in intellectual property cases where there is an issue over the creation date of the defendant's allegedly infringing work. The metadata of an e-mail or electronic document can be the linchpin in establishing or knocking out a defense of independent creation. ESI can also be critical for a plaintiff in a copyright case to establish that the defendant had access to the plaintiff's copyrighted work.

For example, *American Express Co. v. Goetz*, 515 F. 3d 156 (2d Cir. 2008), was a trademark infringement case concerning Amex’s “MY LIFE. MY CARD.” advertising campaign. In affirming the district court’s grant of summary judgment to Amex, the Second Circuit held that the district court had not abused its discretion in determining that Goetz should not be permitted to engage in “wholesale rummaging” through Amex’s electronic records, but only to electronic records pertaining to documents concerning the trademark at issue for which the dates of creation were in question.

Personal Injury

ESI is growing in importance in personal injury cases as well. Text messaging and BlackBerry or iPhone records may show that a driver accused of negligence was preoccupied in the moments leading up to an accident. Similarly, a plaintiff featured in a video or pictures of herself dancing at a party may undercut her claim that her injury has had an impact on her enjoyment of life.

For example, in *Sedie v. U.S.A.*, 2010 WL 1644252 (N.D. Cal. Apr. 21, 2010), a plaintiff’s MySpace page postings had a serious impact on his award in a personal injury case. Sedie sought \$2.5 million in damages for the “hell on earth” he alleged his life had become after an accident with a U.S. Postal Service truck. He claimed he could no longer take part in activities he used to enjoy, such as painting and outdoor activities. However, on his MySpace page, well after the accident, he had a posting stating that he had recently been painting. He ended up getting a judgment in the case for far less than what he had claimed.

Protecting Electronic Information During Litigation

The key steps lawyers can take to protect ESI during litigation are:

1. Educate yourself early on your client’s document retention protocols and capabilities.
2. Communicate immediately upon an action being initiated, or earlier if possible, to the client their duty to preserve ESI, and identify to the client any document retention protocols that should be modified or suspended.

3. Make appropriate secure copies of ESI that might be relevant to the litigation as early on as possible in the litigation, and make backup copies as well that are maintained separately from the initial copies.
4. Maintain clear records of the chain of custody of the preservation of the ESI and the efforts taken to preserve.
5. Regularly follow-up in writing with the client to remind them of their preservation obligations and to insure that they have implemented steps to preserve the appropriate ESI.

It is not only important to protect ESI during litigation (or even before, if a party reasonably anticipates litigation), it is essential. The penalties for failing to comply with document preservation obligations can be severe and can derail a case. At a minimum, e-discovery disputes concerning a failure to preserve documents can distract from the issues in dispute and hamper a case's progress. At worst, a party who fails to preserve relevant documents may be sanctioned by the court. As noted below, sanctions can range from monetary penalties to dismissal of a party's case altogether.

An important step after identifying sources of potentially relevant ESI is determining which sources should be copied or "petrified" so that the ESI is available and intact when it is needed. In some cases, imaging a particular employee's computer hard drive may be necessary. Or, an image of a folder on a company's shared network drive pertaining to the client account at issue may be appropriate.

With regard to e-mails, if a reasonable subset of the e-mails existing on a server can be identified, it is often useful to save that subset in one or several .pst files on DVDs or external hard drives to avoid the possibility of accidental deletion.

One litigant recently learned the hard way that failure to back up a flash drive before sending it for analysis could have severe consequences. In *Wilson v. Thorn Energy LLC*, 2010 WL 1712236 (S.D.N.Y. Mar. 15, 2010), the plaintiffs made loans to and investments in the defendants' petroleum-related projects in Africa, and the defendants agreed to provide an accounting of their use of the plaintiff's funds. However, the defendants kept their only copies of certain documents necessary for the accounting on a USB flash drive. The USB drive failed, however, even before the promise to provide an

accounting happened but after litigation had commenced, and the defendants discarded it. The defendants' attempt to rely on the "safe harbor" provision of Fed. R. Civ. P. 37 (e) (concerning loss of data as a result of good faith, routine operation of an electronic information system) failed, and sanctions ensued—specifically, the defendants were precluded at trial from offering evidence of their financial records or the data allegedly contained on the USB drive. This case clearly illustrates the need to adequately preserve ESI—including by making backup copies of important documents.

The Impact of Failing to Preserve ESI

The most obvious way a failure to preserve and protect ESI can affect the outcome of a litigation is sanctions. Sanctions for spoliation may include attorneys' fees (for conducting depositions or non-party or other discovery to locate alternate sources of "lost" documents, and/or for motion practice concerning spoliation); shifting the costs of locating and reviewing information to the opposing party (particularly for inaccessible sources of ESI, such as backup tapes, the costs for which are usually borne by the requesting party); adverse inference instructions to the jury; or even dismissal.

In *Rimkus*, 2010 WL 645253, employees who preemptively sued their former employer to challenge their restrictive covenants were sanctioned for spoliation of evidence. The Court held that the most severe sanctions—granting default judgment, striking pleadings, or giving adverse inference instructions—might not be imposed without evidence of the spoliators' "bad faith."

In *TR Investors, LLC v. Genger*, 2009 WL 4696062 (Del. Ch. Dec. 9, 2009), the defendant Genger, who was a director of the corporation, together with his computer consultant, intentionally destroyed all information on the unallocated space of a corporation's computer database using wiping software called "SecureClean." Genger did this despite a court order that enjoined the destruction of any company-related documents. The court sanctioned him. As to any affirmative defense or counterclaim he raised, Genger would have to meet an evidentiary burden one level higher than would otherwise be applicable—"clear and convincing" standard instead of by mere preponderance of the evidence. Furthermore, because

Genger's conduct had so seriously compromised his integrity and credibility, he would not be able to rely on his own testimony alone to meet this burden.

Finally, in *Goodman v. Praxair Services Inc.*, 632 F. Supp. 2d 494 (D. Md. 2009), the plaintiff contractor moved for spoliation sanctions based on the corporate defendant's destruction of an employee's laptop. The court found that the corporation willfully destroyed a laptop knowing that it contained evidence relevant to the contractor's claim, including e-mail correspondence, in violation of its duty to preserve evidence. Sanctions were not awarded based on the destruction of other companies' computers, however, because there was insufficient evidence that the materials on those computers were relevant to the contractor's claim.

As technology advances, ESI storage capacities will continue to grow and develop, making ESI storage less and less costly and more and more accessible. Attorneys must make themselves familiar with how clients store their information at the outset of any litigation. It is no longer enough to know where the boxes are stored. Now, key employees who created and/or accessed potentially relevant ESI, and information technology professionals who understand the company's ESI storage capabilities and systems, must be interviewed and involved in a company's preservation efforts.

Due to the sheer volume of ESI produced and stored in the ordinary course of business, attorneys must also become familiar with clients' document retention protocols and counsel them on development and adherence to such protocols.

Despite the many recent decisions there are addressing ESI, the courts do not appear to be moving in a new direction. The *Pension Committee* decision, for example, affirms the preservation obligations that parties already had. However, courts are becoming less tolerant of lapses in preservation efforts and are imposing higher expectations on parties to meet, confer, and develop rational, defensible strategies for preservation, collection, and production of ESI.

Key Takeaways

- In order to protect ESI during litigation, attorneys need to educate themselves early on about their client's document retention protocols and capabilities. They need to communicate immediately upon an action being initiated, or earlier if possible, to the client their duty to preserve ESI, and identify to the client any document retention protocols that should be modified or suspended.
- The attorney should make appropriate secure copies of ESI that might be relevant to the litigation as early on as possible in the litigation, and make backup copies as well that are maintained separately from the initial copies.
- The attorney should maintain clear records of the chain of custody of the preservation of the ESI and the efforts taken to preserve, and regularly follow up in writing with the client to remind them of their preservation obligations and to insure that they have implemented steps to preserve the appropriate ESI.

***Michael C. Lasky** is a partner and co-chair of the Litigation Practice Group of Davis & Gilbert LLP. With more than thirty years of litigation experience, he has litigated a broad range of disputes involving complex commercial disputes relating to the purchase and sale of businesses, trade secret matters, intellectual property, the purchase and sale of business, and employment disputes. Mr. Lasky has also handled some of the leading New York cases involving the movement of talent between competitive companies. Electronic discovery and management of electronic records have been a prominent part of many of the litigations handled by Mr. Lasky. He is also a frequent author and speaker on issues affecting financial services and marketing communications. Mr. Lasky is a Phi Beta Kappa and honors graduate of Rutgers College and Rutgers Law School Newark, where he served as editor-in-chief of the Rutgers Law Review.*

***Marc J. Rachman** is a partner in the Litigation Practice Group of Davis & Gilbert LLP and represents clients in a wide variety of complex commercial litigations. His litigation practice focuses on intellectual property litigation, including trademark and copyright infringement, false advertising, entertainment, right of public city, and domain name disputes. In counseling clients, he has developed document retention policies and electronic media retention protocols. Mr. Rachman has argued appeals before the U.S. Court of Appeals for the Second and Ninth Circuits and the Appellate Division of the*

New York State Supreme Court. He is the author of several articles relating to intellectual property and e-discovery matters and has spoken on various topics, including Social Media, Trademark Law, and the Federal Rules of Evidence. Mr. Rachman is a 1993 cum laude graduate from Boston University School of Law.

Acknowledgment: *The authors would like to acknowledge Cheryl M. Plambeck, without whose significant contribution this chapter would not have been possible.*

Cheryl M. Plambeck *is an associate in the Litigation Practice Group of Davis & Gilbert LLP. Her practice involves litigation in both federal and state courts, covering a broad range of general commercial matters, including employment issues, contractual disputes, business torts, and media law. She has defended various corporate clients and their executives in sex, age, disability and other employment discrimination cases. Ms. Plambeck graduated with distinction from both McGill Law School in 2000, where she earned her B.C.L. and LL.B., and from Tulane Law School with her LL.M. (international and comparative law).*

APPENDIX A

D&G CLIENT PRESERVATION LETTER AND MEMO

[DATE]

Client Contact
Client
Client Address

Re: Document Retention Obligations in Connection
with **[Litigation/Subpoena Title]** or **[Pending or
Threatened Government Investigation]**

Dear _____:

We are writing in connection with our representation of the Company (“you,” “your” or the “Company”) in the **[litigation/subpoena with (name of adversary)]** or **[threatened or pending investigation by (name of Government Agency)]** to advise you of the obligations of the Company and its employees concerning the retention of documents relevant to the **[litigation/subpoena]** or **[investigation]**.

As you may be aware, as a result of this **[litigation/subpoena]** or **[investigation]**, the Company and its employees have a duty to preserve all information that is relevant to the issues that have been or may be raised in the **[litigation/subpoena]** or **[investigation]**. **[For investigation – These obligations arise from such laws as the Sarbanes Oxley Act.]** These obligations include preserving not only hard copies of all relevant documents, but also all electronic data that the Company and/or employees have concerning these issues, including emails and information stored on network servers, back-up tapes, computer discs, hard drives on office desktops or laptops, hard drives on employees’ home desktops or laptops used for Company purposes, PDAs and blackberries. The failure to adhere to these obligations could result in **[for litigation/subpoena - sanctions]** or **[for investigation - criminal penalties]** against the Company and/or its employees.

The Company and its employees, therefore, are required to save all information, electronic or otherwise, that is relevant to the pending **[litigation/subpoena] or [investigation]**. This includes all documents in paper and electronic form. Electronic documents include information from network servers, back-up tapes, other electronic storage, computer discs, hard drives on office desktops or laptops, hard drives on employees' home desktops or laptops used for Company purposes, PDAs, blackberries, and any other source that contains information relevant to the pending **[litigation/subpoena] or [investigation]**.

In accordance with these obligations, the Company must immediately send out the attached preservation memorandum to its IT personnel and all employees that may possess relevant information. **[If known - Based upon the information available to us at this time, we believe the following employees may have relevant information concerning the [litigation/subpoena] or [investigation] and thus, should be sent the attached preservation letter: [list employees]. This list may not include all employees with potentially relevant information and you should check your records to determine whether other employees may have relevant information concerning the [litigation/subpoena] or [investigation].]** We ask that the Company also keep a record of who was sent the attached preservation memo. If at a later date we or the Company determine that additional employees may have relevant information concerning the **[litigation/subpoena] or [investigation]**, you should also send to these individuals the preservation memo.

We will also need to speak to the person(s) at the Company firm in charge of electronic data storage. Please provide us with their contact information so that we may go over with them the steps that need to be taken to preserve all forms of electronic data in connection with the **[litigation/subpoena] or [investigation]**.

If you have any questions, please do not hesitate to contact us.

Sincerely yours,

[your name]

**PRIVILEGED AND CONFIDENTIAL ATTORNEY WORK
PRODUCT AND/OR ATTORNEY-CLIENT
COMMUNICATION**

MEMORANDUM

To: Employee **Date:**
From: General Counsel/IT **File No:**
Department/or Other
CC: IT Department/General Counsel
Re: Preservation of Electronic
Documents and Other Information

This memorandum is to inform you that the Company [is or may become] involved in [a litigation with (name of adversary)/subpoena] or [is aware that it is being investigated by a (name of Federal Agency)]. As you may be aware, as a result of this [claim/litigation/subpoena] or [investigation], you and the Company have a duty to preserve all information that is relevant to the issues that may be raised in the [litigation] or [investigation]. This obligation includes preserving not only hard copies of all relevant documents, but also any electronic data you may have concerning these issues, including emails and information stored on network servers, back-up tapes, computer discs, office desktops or laptops, employees' home desktops or laptops used for Company purposes, PDAs and blackberries. The failure to adhere to these obligations could result in [for litigation/subpoena - sanctions] or [for investigation – fines and/or criminal penalties] against you and/or the Company .

As such, you are now required to save all information, electronic or otherwise, that is relevant to the pending **[claim/litigation/subpoena] or [investigation]**. This includes saving information on network servers, back-up tapes, computer discs, office desktops or laptops, home desktops or laptops used for Company purposes, PDAs and blackberries and any other source that contains information relevant to the pending **[claim/litigation/subpoena] or [investigation]**.

Your receipt of this memorandum is solely because the Company has determined that you may possess information relevant to the pending **[claim/litigation/subpoena] or [investigation]** and does not necessarily mean that you will be involved in the **[claim/litigation/subpoena] or [investigation]**. If you have any questions regarding these obligations, please feel free to contact **[name of the individual in charge of document retention for the claim/litigation/subpoena or investigation]**.

APPENDIX B

PRESERVATION CHECKLIST

ELECTRONIC DISCOVERY BEST PRACTICES

Preservation Checklist

When to commence preservation efforts:

Preservation efforts should be commenced at the earliest opportunity after any of the following events:

- Service of a Complaint (if the client is a defendant)
- Service of a subpoena
- Service of a request for documents
- A party reasonably anticipates litigating a claim
- Receipt of notice of a threatened or pending government investigation

Who to contact:

If you do not already have a contact at the client, identify who your contact(s) should be. Often the Chief Financial Officer or another senior-level executive will be your first point of contact. He or she may want to delegate responsibility for document preservation to someone else, particularly if he or she was not directly involved in the matter at issue. Your contact should be a senior-level employee who either has knowledge about the matters at issue in the litigation or investigation or can help you get in touch with those employees who do.

What to do:

- ✓ Send a letter to your client contact describing preservation duties, and enclosing a memo that can be distributed to all employees with potentially relevant information, including employee(s) who will supervise document preservation efforts and IT personnel.

- ✓ Identify senior-level employee(s) responsible for supervising document preservation efforts and senior-level employee(s) in the IT department with an understanding of the client's ESI retention policies and procedures.
- ✓ Identify all other employees who may have potentially relevant information.
- ✓ Confirm that the preservation memo has been circulated to IT and Records departments, as well as to all other employees with potentially relevant information.
- ✓ Schedule discussions with IT, employee(s) responsible for supervising document preservation efforts, and any employee(s) with potentially relevant documents or their supervisor.

Questions to ask:

- (1) These questions can be used to guide discussions with clients in order to make informed decisions and recommendations.

Questions for IT:

Document Retention Protocols:

- Do you have a written document retention protocol for electronic documents?
 - If so, ask for a copy and review it.
 - Ask if they always follow the written protocol or if their practice deviates from it.
 - Recommend any changes necessary to protocols to ensure that potentially relevant documents are not deleted.
 - If not, ask about practices and unwritten protocols concerning retention/deletion of e-mails and other electronic documents.
 - Do you back up e-mails?
 - Do you back up other electronic documents?

- On employees' local computer drives?
- On any shared drive?
- On any other file server?
- How often are back-up copies made?
- Where are back-up copies kept?
- How long are back-up copies kept?
- What is the oldest back-up tape or other back-up copy that you still have?

Understanding the Relevant Systems:

- What kind of computers do employees use?
 - Macs
 - PCs
 - Desktop computers
 - Laptops

E-mail System:

- What e-mail system do you use?
 - Microsoft Outlook
 - Lotus Notes
 - Other
- Has the e-mail system changed in the past (1 year/3 years/5 years or any other relevant period)?
 - When did it change?
 - What happened to employees' e-mails that were on the server at the time of the change?
 - Were they migrated to a new program?
 - Were they deleted?
 - Were they archived and retained?
 - Are there any restrictions on employees' ability to retain e-mails?
 - Date restrictions
 - *E.g.*, are all e-mails older than 180 days automatically deleted?
 - Size restrictions

- *E.g.*, are employees allowed to keep only 500 MB of e-mails at any given time?
- Are these universal restrictions or do different restrictions apply to different groups of employees?
 - *E.g.*, are senior executives allowed unlimited e-mail storage, while junior-level staff are restricted?
- Can employees archive e-mails locally to their computers?
- Are e-mails of former employees ever retained?
 - Under what circumstances
 - Where are they retained?
 - How long are they retained?

Other Electronic Documents:

- Do employees save documents they are working on locally to their computer hard drives?
- Do employees save documents they access or work on to a shared drive?
 - How is the shared drive organized?
 - Is the shared drive searchable?
 - Are there any automatic deletion processes that affect documents on the shared drive?
- Do employees work at home?
 - If so, do they log on to the client's server?
 - Can they access company e-mails from home?
 - Does the company provide employees with laptops or desktop computers to use at home?
- Do employees input information into any special or proprietary programs?
 - *E.g.*, timekeeping programs, payroll programs, accounting programs, sales tracking programs, etc.
- Do employees use instant messaging or other electronic methods of communication (such as Facebook or LinkedIn) in their work?
 - If so, are records of these communications maintained?
 - If so, how, where and for how long?
- What are your in-house search capabilities?

- If I wanted to get all e-mails sent to or from John Doe between January 1 and June 1, 2010, are you able to search and collect only those e-mails?
- If I wanted to get all e-mails referring to Product X, can you run keyword searches across all employees' e-mails on your server?

Questions for Records:

If the client has a records department separate and apart from its IT, questions should include:

- Is there a document retention protocol for storage of hard copy documents?
 - If so, ask for a copy and review it.
 - If not, ask about practices and unwritten rules regarding retention of paper documents.
- Does the company have any offsite paper record storage?
 - If so, what is kept there?
 - How is it organized?
 - How long are records kept offsite?
- Does the company have any records storage facilities on the premises?
 - If so, what is stored there?
 - How is it organized?
 - How long are records kept there?
 - Note that many clients do not have centralized record-keeping facilities on or offsite, but may have file cabinets or other document storage facilities assigned to particular departments or employees.

Questions for individual employees:

Background information:

- Did you do any work that may be relevant to the case/investigation?
- What work did you do?

- Did anyone else do that work?
- Who?
- What was your title?
 - Has that changed over time?
- Who did you report to?
 - Has that changed over time?
- How long have you been with the company?
- How long were you working on the [potentially relevant project/assignment/client/issue]?
- What were your duties and responsibilities for the [potentially relevant project/assignment/client/issue]?

Communications:

- Who did you communicate with, generally, concerning this work?
 - Which co-workers did you communicate with?
 - Which of them are still with the company?
 - If any have left – when did they leave?
 - Did you communicate with any outside vendors, client contacts, etc?
 - Who?
- Did you communicate by e-mails, instant messages, telephone or any other methods?
 - Did you keep copies of these communications or any notes about these communications?
 - Where are these documents now?
- How far back do your e-mails go?
 - Are you a “keeper” or a “deleter”?
 - Do you file your e-mails in relevant subfolders?
- When you work on a document concerning the [potentially relevant project/assignment/client/issue], where do you save it?
- Do you delete these documents?
- Do you still have these documents?
- Are they in any particular file or folder on your computer or the company server?

Hard copy files:

Hard copy files should be copied and the location of original documents should be recorded.

- Do you tend to keep hard copy files concerning the work you do?
- Do you still have any hard copy files concerning the [potentially relevant project/assignment/client/issue]?
 - Where are they now?
 - What do you have?
 - Did you send any of your files concerning the [potentially relevant project/assignment/client/issue] to offsite storage?
 - When?

What to do next:

- Record dates of receipt and distribution of the preservation memo to employees.
- Take steps to reduce the risks associated with accidental loss of data.
 - Consider copying documents to a secure location and/or imaging hard drives.
 - Investigate the costs/practicalities of copying documents to a secure location or imaging the hard drives of all employees with potentially relevant information.
 - In many cases e-mails currently on a server or archived on a user's local drives should be copied to avoid the risk of loss through end-user error at a later time.
 - If not impractical, e-mails of key employees currently on the client's server should be copied to external drives or DVDs.
 - If not impractical, e-mails archived locally on a user's computer should be copied to external drives or DVDs.

- If the volume of e-mails renders copying users' entire collection impractical, keyword searches sufficiently broad to capture all potentially responsive documents may be used to collect an appropriate subset of e-mails for preservation.
- Other electronic documents should also be copied and preserved.
 - Depending on the needs of a particular case, it may be possible to copy electronic documents from shared network drives and local drives to DVDs or external drives for preservation purposes.
 - In some instances an exact image of the document rather than a copy will be necessary.
 - Imaging hard drives is the best way to ensure going forward that no electronic data is destroyed. Once an employee's hard drive is destroyed, there is a preserved record of everything that was on that employee's computer at the time of the imaging.
- Consider restoration of deleted files.
 - Rarely does a Client's IT department know the proper methods to restore deleted files without actually destroying potentially relevant information. It is not worth the risk of losing potentially relevant data to have the Client restore deleted files from a hard drive. Have restoration of deleted files done by an outside vendor.
 - This is different than the restoration of files from back-up tapes, which can be done by the Client if the Client has the necessary resources.
- Follow up with the client and send periodic reminders concerning the obligation to preserve potentially relevant information.
- Promptly inform the client of any change in the scope of documents that must be preserved.

- Ask the client to let you know if any employees previously identified as possessing potentially relevant information are terminated or leave.
 - Before any departing employees' desktop or laptop computers are recycled, discarded, wiped clean or given to other employees to use:
 - Ensure that all potentially relevant information has been copied or imaged.
 - In some cases, it may be necessary to image the entire hard drive.
 - As an alternative, the hard drive may be quarantined, but this may be costlier in the long run than imaging.
 - Collect all potentially relevant information and documents from the employee's hard copy files.

Chain of Custody:

Maintain a written record of the chain of custody of all copies of electronic documents made by client.

- For copies of electronic files burned to disc from a hard drive and hard drive images, make sure there is a record of the date the disk was burned or the image was made, who burned the disc or made the image and from what computer the files were copied or imaged.
- For copies of electronic files burned to disc from a backup tape, make sure there is a record of the description of the back-up tape (e.g., the date the back-up tape was made, what was contained on the back-up tape and the volume name of the back-up tape), who restored the data from the back-up tape and when and who burned the restored data from the back-up tape to disk and when.



ASPATORE

www.Aspatore.com

Aspature Books, a Thomson Reuters business, exclusively publishes C-Level executives (CEO, CFO, CTO, CMO, Partner) from the world's most respected companies and law firms. C-Level Business Intelligence™, as conceptualized and developed by Aspature Books, provides professionals of all levels with proven business intelligence from industry insiders—direct and unfiltered insight from those who know it best—as opposed to third-party accounts offered by unknown authors and analysts. Aspature Books is committed to publishing an innovative line of business and legal books, those which lay forth principles and offer insights that when employed, can have a direct financial impact on the reader's business objectives, whatever they may be. In essence, Aspature publishes critical tools for all business professionals.

Inside the Minds

The *Inside the Minds* series provides readers of all levels with proven legal and business intelligence from C-Level executives and lawyers (CEO, CFO, CTO, CMO, Partner) from the world's most respected companies and law firms. Each chapter is comparable to a white paper or essay and is a future-oriented look at where an industry, profession, or topic is heading and the most important issues for future success. Each author has been selected based upon their experience and C-Level standing within the professional community. *Inside the Minds* was conceived in order to give readers actual insights into the leading minds of top lawyers and business executives worldwide, presenting an unprecedented look at various industries and professions.



ASPATORE