Program: Has Your Email Become a Corporate Record? Section 220 of the Delaware General Corporation Law entitles a stockholder with a proper purpose to inspect corporate books and records “necessary and essential” to achieving that purpose. Historically, board minutes, resolutions and similar documents were sufficient for Section 220 inspections. However, as advancing technology has resulted not only in new forms of electronic records and communications, such as emails and text messages, but the pervasive and ubiquitous use thereof, the Delaware courts have had to address whether these forms of electronic information constitute corporate books and records subject to inspection under Section 220. This panel will discuss the recent case law in the area of books and records inspections and provide practice tips for transactional counsel and litigators from board minute-taking, to corporate record-keeping, to making and responding to Section 220 demands, and to litigating Section 220 actions.

Originating at common law, the right of a stockholder to inspect the books and records of a corporation is well established in Delaware. The common law recognized inspection rights to provide a stockholder a means of “self-protection.” As a part owner, a stockholder was entitled to know the condition of the corporation and how corporate fiduciaries and agents were conducting its business and affairs. The common law right, though, was a qualified one, requiring the stockholder to show that the inspection was for a “proper purpose”—a purpose relating to the stockholder’s interest as an owner of the corporation’s stock, and not for speculative reasons, idle curiosity, or unlawful ends. In addition, a stockholder generally was not entitled to inspect all of the books and records of the corporation, but only those that were “necessary and essential” to accomplish the stockholder’s proper purpose.

At common law, a stockholder’s right of inspection was enforceable through a formalistic and burdensome mandamus procedure in Delaware Superior Court. A stockholder’s right of inspection, however, has been codified in Delaware in some form for more than 100 years. The current statutory provision, 8 Del. C. § 220, provides a summary procedure by which a stockholder with a proper purpose may gain prompt access to corporate books and records or apply to the Delaware Court of Chancery for an order to compel an inspection.

Historically, stockholders infrequently exercised their right to inspect corporate books and records. But beginning about 20 years, the Delaware courts have encouraged (and at times even admonished) stockholders to use books and records inspections as an information-gathering tool before filing breach-of-fiduciary-duty complaints subject to heightened pleading standards. Referred to as one of the “tools at hand,” Section 220 demands have become commonplace and, as a result of recent case law developments, have expanded beyond the derivative context alleging corporate mismanagement so as to now oftentimes precede direct actions by stockholders challenging corporate mergers.

At the same time as books and records demands have become much more prevalent, advances in technology have resulted in new forms and stores of corporate information not traditionally thought of as corporate “books and records.” Consequently, stockholders seeking to exercise their
inspection rights now increasingly demand the production of not only board minutes, resolutions, consents and related materials, but also electronically stored information such as emails and text messages between or among corporate directors and officers.

Mindful that stockholder books and records inspections are not equivalent to comprehensive discovery in a plenary case and should not be used as a means to conduct a “fishing expedition,” the Delaware courts typically have been reluctant to order production of such electronic documents or communications and instead have deemed traditional board-level materials, such as minutes and resolutions, sufficient to satisfy a stockholder’s purpose. But a court’s determination whether certain documents are “necessary and essential” to a stockholder’s purpose is necessarily one that is dependent on the specific facts and circumstances. Further, the Delaware courts will interpret Section 220 “in light of companies’ actual and evolving record-keeping and communication practices.” Thus, if a corporation’s traditional, non-electronic books and records are insufficient to satisfy a stockholder’s proper purpose, then a court will likely order emails and other electronic documents to be produced. As the Delaware Supreme Court observed in a recent case, “[t]oday, emails and other electronic communications do much of the work of the paper correspondence of yore.”

This program will discuss the recent case law in the area of books and records inspections and provide practice tips for transactional counsel and litigators in light of directors’ and officers’ common use of electronic communications to conduct corporate business—from board minute-taking, to corporate record-keeping, to making and responding to Section 220 demands, and to litigating Section 220 actions.
Board of Directors Materials

Discovery and Information Governance Best Practices

Overview

- Board of Directors Materials
- Retention in the Ordinary Course
- Discovery in Litigations and Investigations
- Best Practices
- Hypotheticals
Board of Directors Materials

Materials generated by, prepared for or at the direction of or distributed to, members of the Board of Directors, can include:

- Formal presentations, documents and information
- Meeting minutes
- Informal documents and information exchanged between or with members
- Stored communications of any kind:
  - Email, text messages, instant messages, voicemail, social media posts, letters, faxes and other correspondence
- Notes of any kind:
  - Handwritten, electronic, marginalia on other documents
Retention in the Ordinary Course

- Organizations are not required to retain all Board materials
- Specific categories of Board materials subject to retention duties should be listed in a retention schedule
- Retention should be publicized and enforced

Sample Record and Information Governance Policy

<table>
<thead>
<tr>
<th>Corporate</th>
<th>Retention Duration</th>
<th>Business Need</th>
</tr>
</thead>
<tbody>
<tr>
<td>Board and Shareholder Meetings</td>
<td>Permanent</td>
<td>Business Need</td>
</tr>
<tr>
<td>Committee Meetings</td>
<td>Year created + 10 years</td>
<td>Business Need</td>
</tr>
<tr>
<td>Financial Oversight and Complaints</td>
<td>Date created + 7 years</td>
<td>Business Need</td>
</tr>
<tr>
<td>Policies, Procedures, Manuals, and Guidelines</td>
<td>While active + 10 years</td>
<td>Business Need</td>
</tr>
<tr>
<td>Acquisition files (including Closing documents, Bills of Sale, etc.)</td>
<td>Permanent</td>
<td>Business Need</td>
</tr>
<tr>
<td>Annual and Quarterly Reports</td>
<td>Permanent</td>
<td>Business Need</td>
</tr>
<tr>
<td>Directors’ Compensation Records</td>
<td>7 years after final compensation payment</td>
<td>Business Need</td>
</tr>
<tr>
<td>Memoranda to the Board</td>
<td>Permanent</td>
<td>Business Need</td>
</tr>
<tr>
<td>Minute Books</td>
<td>Permanent</td>
<td>Business Need</td>
</tr>
<tr>
<td>Notices of Shareholder and Board Meetings</td>
<td>Permanent</td>
<td>Business Need</td>
</tr>
<tr>
<td>Shareholder Records</td>
<td>Permanent</td>
<td>Business Need</td>
</tr>
</tbody>
</table>
Discovery in Litigations and Investigations:

- Board of Directors materials are discoverable
- Location of material is not an impediment to discovery
  - Email on another company’s email server or in a personal email account may be discovered
  - Text messages, photos or other information on a smartphone may be discovered
- Potential limits on discovery of Board of Directors materials:
  - Possession, custody or control
  - Relevance
  - Privilege
  - Uniqueness
  - Accessibility
  - Proportionality
Best Practices

- Management sets recordkeeping policy:
  - Board members should be familiar with organization’s policies
  - Board members should use resources provided by management
- Board Portals:
  - Provide dedicated hardware
  - Centralize all Board materials
  - Centralize all Board communications
  - Discourage or prohibit printing
  - Enforce retention schedule in portal
- Paper:
  - Distribute paper materials only to those physically present at Board meeting
  - Collect all materials, hard copy notes, including marginalia on other documents, whether created at the meeting or beforehand by any attendee, on the way out of Board meetings
- Notes:
  - Discourage notetaking and/or limit to portal
Hypotheticals

- Outside Board member sends and receives email from personal email account
- Outside Board member sends and receives email from business account of another organization
- Outside Board member receives email that includes privileged content at his email address at another organization
- Management invites Chief of X to present at Board Meeting; Chief prepares detailed written talking points for use during presentation.
HAS YOUR EMAIL BECOME A CORPORATE RECORD?

ABA BUSINESS LAW SECTION ANNUAL MEETING
CORPORATE GOVERNANCE COMMITTEE
DIRECTOR & OFFICER LIABILITY COMMITTEE
SEPTEMBER 12, 2019  2:30 PM – 4:00 PM
Has Your Email Become A Corporate Record?

- The Context: For years, when dismissing stockholder derivative actions, the Delaware Courts have admonished that stockholder plaintiffs should use the “tools at hand.”
- The plaintiffs’ bar listened – since mid-2000’s, virtually every derivative action is now preceded by a Section 220 books and records demand.
- Why should you care?
  - Litigation Risk
  - Expense
  - The “Rabbit-Hole” Effect
  - Garner-Doctrinal / Attorney-Client Privilege Waiver
Has Your Email Become A Corporate Record?

- We will cover…..

- (1) The Nuts & Bolts of Stockholder Rights To Inspect the Corporation’s Books and Records

- (2) Problems Presented By Corporate Record Keeping In The Electronic Age

- (3) The Legal Framework for Determining When Electronic Records Must Be Produced

- (4) Protective Measures In Books And Records Matters

- (5) Key Take-Aways – Do’s, Don’ts and Don’t You Ever!!
I. Inspection of Books and Records

- Historical Right at Common Law
- Statutory Form and Manner Requirements
- Proper Purpose Requirement
- Necessary and Essential Scope
- Director Inspection Rights
- Confidentiality Agreements and Limitations and Conditions on Inspection
Historical Right at Common Law

- Long recognized at common law, a stockholder of a Delaware corporation has a qualified right to inspect the books and records of the corporation.
- Inspection rights viewed at common law as a form of stockholder “self-protection.”
- A stockholder’s common law right of inspection could not be taken away except by statutory enactment.
- The common-law right of inspection was enforceable only through issuance of a writ of mandamus from Superior Court compelling corporation to permit inspection.
- The writ of mandamus was an extraordinary remedy that would only issue if the stockholder clearly established an entitlement to the requested inspection.
- This required the stockholder to show a “proper purpose.”
- Stockholder permitted to inspect documents “essential and sufficient” for purpose.

Statutory “Form and Manner” Requirements

- “upon written demand”
- “under oath”
- “stating the purpose thereof”
- “where the stockholder is other than a record holder of stock … the demand under oath shall”
  - “state the person’s status as a stockholder”
  - “be accompanied by documentary evidence of beneficial ownership of the stock, and”
  - “state that such documentary evidence is a true and correct copy of what it purports to be.”
- “where an attorney or other agent … seeks the right to inspection, the demand under oath shall be accompanied by a power of attorney …”
- “directed to the corporation at its registered office in this State or at its principal place of business.”
- Delaware courts require “strict adherence” to form and manner requirements.

“Proper Purpose” Requirement

- When seeking to inspect books and records, a stockholder bears the burden of establishing that the inspection is for a “proper purpose.”
- A “proper” purpose is one “reasonably related” to “interest as a stockholder.”
- A stockholder’s primary purpose must be proper and must not be adverse to the best interests of the corporation. If the stockholder’s primary purpose is proper, any secondary purpose or ulterior motive is irrelevant.
- Examples of purposes the Court has recognized as proper include:
  - Valuing one’s shares in the corporation;
  - Examining the independence and disinterestedness of directors; and
  - Investigating possible mismanagement or fiduciary breaches.
- If a stockholder’s purpose for inspection is to investigate possible wrongdoing, the stockholder must present some credible evidence to warrant further investigation.
  - The “credible basis” standard sets “the lowest possible burden of proof.”

What Is Not A “Proper Purpose”? 

- What are examples of situations that do not give rise to a “proper” purpose?
  - Mere curiosity or suspicion
  - Disagreement with a business decision
  - Poor financial performance
  - Failure of a transaction
  - Circumvent a discovery stay in pending litigation
  - Intent to bring suit that is barred or exculpated
  - Intent to bring suit without standing
  - Buying stock to pursue a claim
  - Lawyer-driven purposes

“Necessary and Essential” Scope

- The scope of a stockholder’s inspection is limited to the books and records “necessary and essential” to satisfy the stockholder’s stated proper purpose.
- Documents are “necessary and essential” if they address the “crux of the shareholder’s purpose” and the information is “unavailable from another source.”
- The burden is on the stockholder to show each category of requested books and records is “essential to the accomplishment” of the stockholder’s stated purpose.
- Section 220 is “not meant as a replacement for discovery under Rule 34” and does not permit “wide ranging discovery” generally available in plenary litigation.
- Stockholders must make books and records demands with “rifled precision.”
- Scope of inspection can include the books and records of a subsidiary in certain circumstances. Scope of inspection also may include officer-level documents and documents received by the corporation from third parties.

Director Inspection Rights

- Delaware common law also recognized a corporate director’s right to inspect the corporation’s books and records. This right is now codified in 8 Del. C. § 220(d).
- The rationale for this right is that a director is charged with fiduciary obligations to the corporation and the stockholders, and therefore must have access to the corporate books and records to fulfill those duties.
- Different standards than those applicable to stockholder inspections, including the form and manner of demand, the burden of proof, and the scope of inspection:
  - Demand need not be written.
  - No five business day waiting period to file complaint.
  - Director makes out a prima facie case by showing that he is a director, he has demanded inspection, and his demand has been refused by the corporation.
  - The burden of proof is on the corporation to prove an improper purpose.
  - The inspection is not limited to “necessary and essential” books and records, but rather is “essentially unfettered” in scope, extending to privileged material.

(2) Problems Presented By Corporate Record Keeping In The Electronic Age

- Issues Arising In The Electronic Age
- Record Retention Obligations
- Record Management Policies
- Board-Level Best Practices
Records that Must Be Maintained

- Record Retention obligations in the ordinary course of business are generally driven by (a) law and regulation in specific industry or business function or (b) business need.
- Format (electronic v. paper; email v. memo) is irrelevant; content determines retention.
- An effective information governance program should contain Information Lifecycle Management policies including:
  - Retention policy
  - Retention schedule
  - Data Privacy
  - Information Security
  - Acceptable Use
  - Legal Hold
  - Disposition
Retention in the Ordinary Course

- Organizations are not required to retain all Board materials
- Specific categories of Board materials subject to retention duties should be listed in a retention schedule
- Retention should be publicized and enforced
# Sample Record and Information Governance Policy

<table>
<thead>
<tr>
<th>Corporate</th>
<th>Record Type</th>
<th>Retention Period</th>
<th>Business Need</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate</td>
<td>Board and Shareholder Meetings</td>
<td>Permanent</td>
<td>Business Need</td>
</tr>
<tr>
<td>Corporate</td>
<td>Committee Meetings</td>
<td>Year created + 10 years</td>
<td>Business Need</td>
</tr>
<tr>
<td>Corporate</td>
<td>Financial Oversight and Complaints</td>
<td>Date created + 7 years</td>
<td>Business Need</td>
</tr>
<tr>
<td>Corporate</td>
<td>Policies, Procedures, Manuals, and Guidelines</td>
<td>While active + 10 years</td>
<td>Business Need</td>
</tr>
<tr>
<td>Corporate</td>
<td>Acquisition files (including Closing documents, Bills of Sale, etc.)</td>
<td>Permanent</td>
<td>Business Need</td>
</tr>
<tr>
<td>Corporate</td>
<td>Annual and Quarterly Reports</td>
<td>Permanent</td>
<td>Business Need</td>
</tr>
<tr>
<td>Corporate</td>
<td>Directors' Compensation Records</td>
<td>7 years after final compensation payment</td>
<td>Business Need</td>
</tr>
<tr>
<td>Corporate</td>
<td>Memoranda to the Board</td>
<td>Permanent</td>
<td>Business Need</td>
</tr>
<tr>
<td>Corporate</td>
<td>Minute Books</td>
<td>Permanent</td>
<td>Business Need</td>
</tr>
<tr>
<td>Corporate</td>
<td>Notices of Shareholder and Board Meetings</td>
<td>Permanent</td>
<td>Business Need</td>
</tr>
<tr>
<td>Corporate</td>
<td>Shareholder Records</td>
<td>Permanent</td>
<td>Business Need</td>
</tr>
</tbody>
</table>
Information Governance Reference Model (IGRM)

Linking duty + value to information asset = efficient, effective management

**Duty:** Legal obligation for specific information

**Value:** Utility or business purpose of specific information

**Asset:** Specific container of information
Best Practices

- Management sets recordkeeping policy:
  - Board members should be familiar with organization’s policies
  - Board members should use resources provided by management

- Board Portals:
  - Provide dedicated hardware
  - Centralize all Board materials
  - Centralize all Board communications
  - Discourage or prohibit printing
  - Enforce retention schedule in portal

- Paper:
  - Distribute paper materials only to those physically present at Board meeting
  - Collect all materials, hard copy notes, including marginalia on other documents, whether created at the meeting or beforehand by any attendee, on the way out of Board meetings

- Notes:
  - Discourage notetaking and/or limit to portal
(3) The Legal Framework for Determining When Electronic Records Must Be Produced

- Highly contextual inquiry
- Turns on:
  - Nature and purpose of the request
  - How company maintained records (formal records vs. informal communications)
  - Availability of other records from other sources
  - Practices of the relevant custodians
Seminal decision granting access to emails in a Section 220 Production is Indiana Electrical Workers Pension Trust Fund IBEW v. Wal-Mart Stores, Inc., C.A. No. 7779-CS (Del. Ch.), aff’d, 95 A.3d 1264 (Del. 2014).

- Did not directly rule emails are corporate records; rather ordered production of private communications between officers and directors regarding an internal bribery scandal where plaintiff was seeking information on knowledge and culpability of directors to determine demand futility.
- Directors’ personal devices and home computers were equally subject to Section 220 inspection.
- “Just because it’s at home, doesn’t make it your own”
Are Emails (Texts, Snapchat …) Corporate Records?

  - Being stored on a company server ≠ company record
  - Email communications become a “corporate record” “to the extent that they affect the corporation’s rights, duties and obligations.” *Id.* at *11 n.116.
- 3-part Chammas Test re: When to Produce Emails:
  1) Stockholder states a Proper Purpose;
  2) The communication rises to level of corporate record because it affects rights, duties and obligations of company; and
  3) The request was sufficiently tailored to the specific books and records to achieve the proper purpose.

Are Emails the Only or Best Records?

- Lack of formal Board documents or customary usage of email to conduct business will factor into Court’s analysis to order the production of emails. See KT4 Partners LLC v. Palantir Technologies, Inc., 203 A.3d 738 (Del. 2019).

- Evidence of officer or director preference to conduct business via email will weigh in favor of Court ordering production of emails. In re Facebook, Inc. Section 220 Litigation, 2019 WL 2320847, *18 n.185 (Del. Ch. May 30, 2019) (Stockholder had sufficient documentation to show directors conducted business and communicated by email, rendering these documents a necessary component in investigation of mismanagement).
(4) Protective Measures
In Books And Records Matters

- So you have agreed to, or the Chancery Court has ordered, production of books and records. Besides litigation risks, what concerns should you have, and is there anything you can do about them?
- Specifically, how do you protect against ….
  - Breaches of Confidentiality?
  - Leakage?
  - Improper use of records?
  - Forum shopping?
  - Cherry-picking?
Confidentiality Agreements

8 Del. C. § 220(c) – “The Court may, in its discretion, prescribe any limitations or conditions with reference to the inspection, or award such other or further relief as the Court may deem just and proper.”

“The Court may order the corporation to [produce documents] . . . On condition that the stockholder first pay . . . the reasonable cost of obtaining and furnishing [the documents] and on such other conditions as the court deems appropriate.”


Previously, “One common limitation is to condition production on the stockholder entering into a confidentiality agreement. Although once novel, now “[t]here is a presumption that the production of books and records pursuant to section 220 should be ‘conditioned upon a reasonable confidentiality order.’” Amalgamated Bank v. Yahoo! Inc., 132 A.3d 752, 796-97 (Del. Ch. 2016).

While companies “will often be able to demonstrate that some degree of confidentiality is warranted where they are asked to produce nonpublic information,” there must be an assessment of “benefits and harms when determining the initial degree and duration of confidentiality.” Tiger, 2019 WL 3683525, at *4.
Confidentiality Agreements

- A “corporation need not show specific harm that would result from disclosure” before requiring an undertaking, but there should not be a reflexive conclusion that all information will be confidential. *Id.*
- *See Kosinsky v. GGP Inc.*, 2019 WL 4052054, *10 (Del. Ch. Aug. 28, 2019)* (“[T]he record does not reflect any negotiations concerning whether the documents to be inspected should be subject to reasonable confidentiality restrictions – *this Court does not presume that they should be.*”).
- Corporate fiduciaries need not sign confidentiality undertakings, they are “already [] obliged to protect the Company’s information.” *Schnatter v. Papa John’s Int’l, Inc.*, 2019 WL 194634, *17 (Del. Ch. Jan. 15, 2019).
Specific Protections in Confidentiality Agreements/Court Orders For Production

**Preventing Leakage:** Prevent the stockholder from inadvertently “discovering” claims based upon topics unrelated to the specific area of inquiry stated in the demand

- Expressly permit redactions of all material not relevant to the demand.

**Preventing Improper Use:**

- Cannot use the production to aid other litigation pending between the parties.
  
  See e.g., *OpenTV, Inc. v. Broadband iTV, Inc.*, C.A. No. 2018-0346-SG (Order) (Del. Ch. Sept. 24, 2018) ("Stockholder may not use the Produced Documents in the pending litigation between the parties captioned Broadband iTV, Inc. v. OpenTV, Inc., Case No. CGC 17-561922 (Cal. Super. Ct.), Case No. 17-cv-0647-SK (N.D. Cal.) . . . Unless the materials first are obtained through other means such as formal discovery in that action.").

- *Henshaw v. American Cement Corp.*, 252 A.2d 125, 130 (Del. Ch. 1969) (Allowing a stockholder’s attorney in fact to review Section 220 production was inappropriate where the counsel was also an adversary to the company “back-door discovery unbound by work-product, privilege or any other limitation upon discovery” and stockholder’s right to have counsel who is a current litigation adversary must “give way to protection of the corporate interest.”).
Specific Protections in Confidentiality Agreements/Court Orders For Production

- *But see Schnatter v. Papa John’s Int’l, Inc.*, 2019 WL 194634, *18 (Del. Ch. Jan. 15, 2019) (rejecting that stockholder’s counsel should be prohibited from seeing any documents produced in 220 Production simply because they represent him in other litigation pending between the parties, “[b]arring Schnatter’s lawyers from helping him with the inspection would be prejudicial to Schnatter because it would require him to retain new counsel to perform that task.”).


Preventing Forum Shopping

- Jurisdictional Use Restrictions: Require that if plenary action is asserted based on the production, such suit must be filed in Delaware or another specified forum.

- Permitted only on a case-by-case basis where jurisdiction limitations will promote the company’s legitimate interests in having consistent rulings, where it promotes judicial economy and could reduce costs (eliminate multi-jurisdictional and overlapping rulings), but not where Delaware courts might not be able to assert personal jurisdiction over a necessary defendant, leaving a stockholder without a full remedy. *See KT4 Partners LLC v. Palantir Technologies, Inc.*, 203 A.3d 738, 758-66 (Del. 2019)
Specific Protections in Confidentiality Agreements/Court Orders For Production

Preventing Cherry-Picking

- The incorporation-by-reference condition (or the “Incorporation Condition”) was approved first in *Amalgamated Bank v. Yahoo! Inc.*, 132 A.3d 752 (Del. Ch. 2016).
  - “Yahoo asks that this court condition any further production on Amalgamated incorporating by reference into any derivative action complaint that it files the full scope of the documents Yahoo has produced or will produce in response to the Demand. . . Yahoo’s request is granted, and further production is conditioned on Amalgamated agreeing that the entirety of Yahoo’s production in response to the Demand is incorporated by reference in any derivative action complaint it files relating to the subject matter of the demand.” *Id.* at 796.
  - “[T]he Incorporation Condition protects the legitimate interest of both Yahoo and the judiciary by ensuring that any complaint that Amalgamated files will not be based on cherry-picked documents.” *Id.* “The doctrine limits the ability of the plaintiff to take language out of context, because the defendants can point the court to the entire document . . . [and] also enables courts to dispose of meritless complaints at the pleading stage.” *Id.*
  - “In the end, the only effect of the Incorporation Condition will be to ensure that the plaintiff cannot seize on a document, take it out of context, and insist on an unreasonable inference that the court could not draw if it considered related documents.” *Elow v. Express Scripts Holding Co.*, 2017 WL 2352121, *9 (Del. Ch. May 31, 2017).
Specific Protections in Confidentiality Agreements/Court Orders For Production

Trading Restrictions?

- In at least two cases, the Court of Chancery has rejected attempts by a publicly traded defendant corporation to impose trading restrictions on a stockholder in order to permit the stockholder to inspect the company’s books and records:
Key Take-Aways
Do’s, Don’ts & Don’t You Ever!!

Records & Information Policies
- Do create and enforce a Records Retention Policy
- Do create and enforce a Records and Information Management Policy
- Do Not expect that your company will be able to produce a Rule 30(b)(6) witness who will be able to explain your record-keeping without well-written policies

Board Materials
- Do maintain clear rules and requirements regarding the retention of Board Materials that results in only one official corporate record of Board action
- Do use Board portals
- Do Not permit directors to take Board Materials outside the boardroom
**Key Take-Aways**

**Do’s, Don’ts & Don’t You Ever!!**

**Board Materials**
- **Do** draft Board minutes with sufficient detail so as to demonstrate the Board’s diligence, deliberations and decisions.
- **Do Not** draft Board minutes so cryptically that it cannot be determined that the directors fulfilled their fiduciary obligations.
- **Do** provide clear guideposts in Board materials that identify privileged advice.
- **Do Not** expect that the associate reviewing your Board Materials years after the fact will recognize all privileged discussions.

**Official Means Of Communication**
- **Do** create and enforce strict policies regarding the means by which business is conducted, especially at the Board and senior management level.
- **Do Not** permit outside directors to conduct all Board business using Board Portals or emails on the company’s server.
- **Do Not Ever** permit senior management or the company’s officers and directors to conduct business outside of official channels *(i.e. other than company-server email)*.
Key Take-Aways
Do’s, Don’ts & Don’t You Ever!!

Responding To Section 220 Demands

- **Do** engage counsel the moment you receive a Section 220 demand for books and records
- **Do Not** allow five business days to pass without responding
- **Do Not Ever** attempt to respond or defend against a Section 220 demand without the assistance of experienced counsel!!
Thank You

Michael D. Blanchard
Morgan, Lewis & Bockius LLP
Tel: (617) 951-8061 & (860) 240-2945
Email: michael.blanchard@morganlewis.com

Tess Blair
Morgan, Lewis & Bockius LLP
Tel: (215) 963-5161
Email: tess.blair@morganlewis.com

Patricia L. Enerio
Heyman Enerio Gattuso & Hirzel LLP
Tel: (302) 472-7303
Email: penerio@hegh.law

Christopher N. Kelly
Potter Anderson & Corroon LLP
Tel: (302) 984-6178
Email: ckelley@potteranderson.com
When Must E-mails Be Produced in DGCL Section 220 Books and Records Actions?

By: Michael Blanchard

| August 20, 2019

IN BRIEF

- As technological advances have expanded the range of media used to conduct business, the law has also evolved regarding access to e-mail, text messages, and other forms of communication as books and records of the corporation.
Although still evolving, some general principles have emerged that generally guide when the Delaware courts will permit access to electronic communications in section 220 proceedings. Producing e-mails in a books and records case cannot always be avoided, but there are steps corporations can take to mitigate the risk.

Since common law, stockholders have enjoyed a qualified right to inspect the corporation’s “books and records” for any “proper purpose”—i.e., a purpose reasonably related to the stockholder’s interests as a stockholder. Codified in state corporation statutes such as section 220 of the Delaware General Corporations Law (DGCL), these stockholder inspection rights were exercised infrequently until the Delaware courts began to encourage stockholders to utilize these “tools at hand” to obtain information necessary to plead demand excusal in derivative actions. As the Delaware Supreme Court noted in the seminal decision of Rales v. Blasband: “Surprisingly, little use has been made of section 220 as an information-gathering tool in the derivative context.” 634 A.2d 927, 935 n.10 (Del. 1993). Over the last 20 years, “Delaware courts have encouraged stockholders to use the ‘tools at hand’ (e.g., Section 220) to gather information before filing complaints that will be subject to heightened pleading standards.” Lavin v. West Corp., 2017 WL 6728702, at *9 (Del. Ch. Dec. 29, 2017). The significant increase in section 220 litigation over the last decade is a testament to the plaintiffs’ bar heeding the Delaware courts’ admonitions.
At the same time that section 220 books and records demands have become commonplace, rapid technological advances have driven the proliferation of the forms of media in which corporate information is kept, including, for instance, e-mails, text messages, and other electronic communications and records not traditionally viewed as a corporation’s “books and records.” The issue is only further complicated by the fact that officers’ and directors’ use of personal computers, smartphones, and personal e-mail accounts potentially renders communications beyond the direct control of the corporations whom the officers and directors serve. Until relatively recently, Delaware courts have been hesitant to compel the production of such “nontraditional” books and records in section 220 litigation, given that the extant jurisprudence dictates that a section 220 summary proceeding is far from coextensive in scope with Rule 34 discovery, and a stockholder is only entitled to those books and records deemed “necessary and essential” to achieving a proper purpose. Typically, board minutes, resolutions, and the like are deemed sufficient because the courts are mindful that a stockholder’s inspection rights must be balanced against the potential for burdensome and abusive “fishing expeditions” that mirror discovery requests in plenary corporate litigation. Nonetheless, as technological advances have expanded the range of media used to conduct business, the law has also evolved regarding access to e-mail, text messages, and other forms of communication as books and records of the corporation. Although still evolving, some general principles have emerged that generally guide when
the Delaware courts will permit access to electronic communications in section 220 proceedings.

Who cares? Corporations and their officers and directors absolutely should. Section 220 demands have become virtually a necessary prerequisite to any stockholder derivative action, and the books and records that stockholders receive and use to draft their complaint can be outcome-determinative on a motion to dismiss. Whereas board minutes and more “formal” corporate records will allow little room for “creative interpretation” by the plaintiffs’ bar, the same cannot be said of e-mail communications where plans and decisions are informally deliberated in real time, perhaps satirically or within a context that may not be evident when portrayed with hindsight by counsel whose objective is to prove a breach of fiduciary duty. Although producing e-mails in a books and records case cannot always be avoided, there are steps corporations can take on a clear day to mitigate the risk.

The seminal decision granting access to e-mails is a 2013 nonpublished transcript ruling, Ind. Elec. Workers Pension Tr. Fund IBEW v. Wal-Mart Stores, Inc., 7779-CS, at 97–98 (Del. Ch. May 20, 2013) (Strine, C.), which ironically does not directly address the issue of whether e-mails are corporate records subject to section 220 inspection rights. In Wal-Mart, then-Chancellor Strine ordered the production of private communications between officers and directors concerning an alleged bribery scandal under investigation by the plaintiff. In the process, the issue arose as to whether e-mails and electronic documents created or maintained on personal devices were the appropriate subject of a
section 220 demand. The court drew no
distinctions between e-mails and documents
created by employees upon their personal devices
verses those generated within the company’s
official systems, concluding that where the
documents were created or maintained was not
controlling: “In terms of this issue of the home
devices . . . if you use your home computer to
handle Wal-Mart information, I don’t think that
many companies would believe that . . . that makes
it their personal information.” Given that the
e-mails were deemed corporate records necessary
for the plaintiff to conduct its investigation, they
were to be produced irrespective of where they
were physically created or maintained. Although
the unpublished Wal-Mart decision did not directly
address when the production of e-mails is
appropriate in a section 220 action, its affirmance
on appeal was routinely cited by the plaintiffs’ bar
for that principle.

The issue arose again in Chammas v. Navlink, Inc.,
2016 WL 767714 (Del.Ch. 2016), a case involving a
director’s demand for books and records pursuant
to the more expansive rights that directors have as
compared to stockholders. In Chammas, the
director plaintiff sought to “investigate whether
‘the other members of the Board and management
are excluding them from board business and
related communications,’ including emails prior to
Board meetings and alleged Secret Meetings.”
Consistent with Wal-Mart, Vice Chancellor Noble
first observed that whether a document or
communication is stored on the company’s servers
is “not necessarily determinative of whether it
constitutes a book or record of the company.”
More important, the court concluded, is whether
the book or record must be “in the possession or
control of the corporation.” Second, recognizing the importance of burden considerations in the section 220 context, the court disclaimed that although its “holding is not to be interpreted as a blanket prohibition against inspection of private communications among directors, subjecting Section 220 proceedings to such broad requests, even by directors, runs contrary to the summary nature of a Section 220 proceeding.” Finally, the court observed that the books and records of the company are “those that affect the corporation’s rights, duties, and obligations . . . .” The court’s ultimate rejection of the demand for e-mails turned on the insufficiency of the plaintiff’s evidence of wrongdoing to warrant their production: “Mere suspicions of pre-meeting collusion among board members or board members and management, in the context of a Section 220 action, is insufficient to compel the production of private communications between such officers and directors . . . .”

The same year Chammas was decided, Vice Chancellor Laster analyzed whether e-mails may be within the scope of books and records obtainable pursuant to section 220. In Amalgamated Bank v. Yahoo! Inc., 132 A.3d 752 (Del. Ch. 2016), a stockholder sought to investigate the hiring of Yahoo’s chief operating officer, and in that connection sought e-mails from the company’s CEO. The court began its analysis by categorically rejecting the argument that e-mails are per se beyond section 220’s scope. Vice Chancellor Laster observed the evolution of corporate record-keeping and the modern reality that virtually all books and records are now kept electronically: “Limiting ‘books and records’ to physical documents ‘could cause Section 220 to become
obsolete or ineffective.” The court then relied upon *Wal-Mart* to reject the argument that the company’s search for documents would be limited to the company’s devices, as opposed to a custodian’s personal device, holding that “a corporate record retains its character regardless of the medium used to create it.” As for the test to determine whether e-mails must be produced, the court limited itself to a single consideration: “As with other categories of documents subject to production under Section 220, what matters is whether the record is essential and sufficient to satisfy the stockholder’s proper purpose, not its source.”

A few years later in *Schnatter v. Papa John’s International, Inc.*, 2019 WL 194634 (Del. Ch. 2019), Chancellor Bouchard addressed the test suggested in *Chammas* as to whether e-mails (or any documents) are deemed books and records of the company—i.e., whether they are “those that affect the corporation’s rights, duties, and obligations . . . .” The defendant in *Papa John’s* resisted production of e-mails between directors discussing former director Schnatter, citing *Chammas* and claiming that “Schnatter is just curious about what his fellow fiduciaries were saying about him.” The court rejected the argument because the scope of documents ordered to be produced would be limited to those related to the plaintiff’s proper purpose, thus satisfying the standard. Commenting further, Chancellor Bouchard then effectively agreed with Vice Chancellor Laster’s reasoning for producing e-mails as articulated in *Yahoo*, albeit qualified by consideration of the additional costs inherent in producing electronic communications:
A further word is in order regarding emails and text messages from personal accounts and devices. The reality of today’s world is that people communicate in many more ways than ever before, aided by technological advances that are convenient and efficient to use. Although some methods of communication (e.g., text messages) present greater challenges for collection and review than others, and thus may impose more expense on the company to produce, the utility of Section 220 as a means of investigating mismanagement would be undermined if the court categorically were to rule out the need to produce communications in these formats.

Citing then-Chancellor Strine’s decision in Walmart, the court held that “if the custodians identified here . . . used personal accounts and devices to communicate about changing the Company’s relationship with Schnatter, they should expect to provide that information to the Company.” Expressly disclaiming the promulgation of any bright-line rule, Chancellor Bouchard grounded the analysis in “balanc[ing] the need for the information sought against the burdens of production and the availability of the information from other sources, as the statute contemplates.”

If there were any question about whether e-mails are properly within the scope of section 220 demands, the Delaware Supreme Court resolved it in KT4 Partners LLC v. Palantir Technologies Inc., 203 A.3d 738 (Del. 2018). In Palantir, after a potential sale of the company fell through because
Palantir allegedly thwarted the deal and KT$ sought information pursuant to its far-reaching rights under an “Investors Rights Agreement,” Palantir allegedly amended the agreement to curtail KT4’s rights. KT4 made a demand to inspect Palantir’s books and records under section 220 of the DGCL for the purpose of investigating “fraud, mismanagement, abuse and breach of fiduciary duty.” Palantir rejected the demand, and KT4 commenced a section 220 action in the Delaware Court of Chancery. Following trial, Vice Chancellor Slight held that KT4 had shown a proper purpose of investigating potential wrongdoing in multiple areas, including Palantir’s amendment of the Investors’ Rights Agreement in ways that “eviscerated” KT4’s contractual information rights after KT4 sought to exercise those rights. The court specifically held that KT4 was entitled to “all books and records relating to” the amendments to the Investors’ Rights Agreement. After the parties were unable to agree on whether the books and records to be produced were to include e-mails, the court issued a final order that excluded e-mails from the documents that Palantir would be required to produce. The court reasoned in part that e-mails were not essential to fulfill KT4’s stated investigative purpose, based on the (mistaken) understanding that Palantir possessed and would produce formal board-level documents relating to the amendments of the Investors’ Rights Agreement, rendering a further production of e-mail unnecessary for KT4’s purpose.

KT4 appealed the Court of Chancery’s ruling. Importantly, on appeal, Palantir conceded that other than the amendments to the Investors’ Rights Agreement themselves, responsive nonemail documents did not exist, and that e-mails
related to the amendments did exist. The Delaware Supreme Court held that the e-mails plaintiff sought were necessary and essential to investigating the alleged wrongdoing because the defendant admitted other, more traditional forms of books and records did not exist. Insofar as being required to produce e-mails was concerned, the Supreme Court viewed Palantir’s obligation as a self-inflicted wound. As the Supreme Court made clear, “if a company observes traditional formalities, such as documenting its actions through board minutes, resolutions and official letters, it will likely be able to satisfy a Section 220 petitioner’s needs solely by producing those books and records.” The court conversely cautioned that “if a respondent in a § 220 action conducts formal corporate business without documenting its actions in minutes and board resolutions or other formal means, but maintains its records of the key communications only in emails, the respondent has no one to blame but itself for making the production of those emails necessary.”

***

The foregoing cases illustrate several principles inherent in any analysis of whether electronic communications will be ordered produced in section 220 litigation. First, electronic communications are deemed corporate records that may be ordered in section 220 proceedings, but only to the extent that they are “necessary and essential” to the plaintiff’s investigation. Second, whether or not the electronic communications reside on the corporation’s servers or personal devices, if they are necessary and essential to the plaintiff’s investigation, they may subject to an order compelling production. Third, although
e-mails may be ordered to be produced in section 220 litigation, the cost and burden of such a production will weigh considerably in the court's final determination. And finally, Palantir serves as an admonition to corporate boards and their counsel to be mindful to observe corporate formalities and appropriately document board meetings and actions through minutes, resolutions, and other official materials, and avoid conducting "formal corporate business . . . through informal electronic communications." Absent proper recordkeeping and formal documentation of the board’s decisions, there is risk that a corporate respondent in a section 220 action may be ordered to produce e-mails as “necessary and essential” to satisfying a stockholder’s books and records demand.

---

Mr. Blanchard is a partner at Morgan, Lewis & Bockius LLP. He represents clients in all facets of shareholder litigation, class actions, securities enforcement matters, investigations, and business disputes. The views expressed by the author are his alone and are not the views of Morgan Lewis or the firm’s clients. This article is for information purposes only and does not constitute legal advice.

---

ABOUT THE AUTHOR

**Michael Blanchard**

Mr. Blanchard is a partner at Morgan, Lewis & Bockius LLP. He represents clients in all facets of shareholder litigation, class actions, securities enforcement matters, investigations, and business...

+ Follow
ACKNOWLEDGMENTS

The eData practice at Morgan Lewis was founded in 2004, just two years before the Federal Rules of Civil Procedure (Federal Rules) were amended to accommodate the growing role of electronically stored information in the discovery process.

Even before eData and the amendments to the Federal Rules, our lawyers were among the few in our profession focused on this extraordinarily challenging practice area. And as this area of the law continues to grow and evolve, so has the eData practice, which has matured into a global practice group comprising more than 100 lawyers, 50 technologists, five dedicated discovery management centers, two data centers, and an offshore review team.

When we issued the initial *Deskbook*, it was our first attempt to gather the considerable knowledge and experience of the eData team and summarize it in a volume that would be useful to our colleagues and clients.

The second edition resulted in a substantial reorganization, following more closely the Electronic Discovery Reference Model (EDRM), as well as a comprehensive update to capture changes in the law and the evolution of this field. This area of the law continues to evolve, leading to this third edition. Exciting changes have occurred in the recent past including the 2015 Amendments to the Federal Rules and the rapidly evolving changes to the European Data Protection Laws and related obligations to collect data outside the United States. The third edition adds considerations and guidance related to information governance, social media and Data Privacy in keeping with recent and ongoing legal and technical developments and trends.

This *eData Deskbook* – Third Edition captures the best practices, practical advice, and experience of its contributors, to whom special thanks and acknowledgment must be given: Jennifer Mott Williams, Tara Lawler, and Lorraine Casto.

To our clients and prospective clients, we hope this *eData Deskbook* proves useful to you, and we look forward to working with you.

Tess Blair
Editor
# TABLE OF CONTENTS

## CHAPTER 1 Introduction to eDiscovery ................................................................. 1

1.1 The World of eDiscovery .................................................................................. 1

1.2 Legal Overview ............................................................................................... 2

1.2.1 The 2015 Amendments to the Federal Rules of Civil Procedure ............... 2

1.3 Ethical Implications of eDiscovery .................................................................... 6

1.3.1 The ABA Model Rules of Professional Conduct ........................................ 6

1.4 The Electronic Discovery Reference Model ....................................................... 9

## CHAPTER 2 Information Governance .................................................................. 13

2.1 The Basic Questions ......................................................................................... 15

2.1.1 The Legal and Regulatory Landscape ....................................................... 15

2.1.2 Data Assessment .................................................................................... 17

2.2 Programs and Policies ..................................................................................... 18

2.2.1 Retention Programs .............................................................................. 18

2.2.2 ESI Policies .......................................................................................... 22

2.2.3 Technological Solutions ........................................................................... 25

2.2.4 eDiscovery Readiness .......................................................................... 26

2.2.5 Training and Implementation .................................................................... 26

2.2.6 Audit ..................................................................................................... 27

2.2.7 Refreshing Retention Schedules .............................................................. 27

## CHAPTER 3 Identification and Preservation ....................................................... 29

3.1 When Does a Duty to Preserve Arise? .............................................................. 29

3.2 What Must Be Preserved? ............................................................................... 33

3.2.1 Guidance from the Federal Rules ............................................................ 33

3.2.2 “Electronically Stored Information” and Its Potential Sources ................ 34

3.2.3 Possession, Custody, or Control ............................................................... 38

3.2.4 Limitations on What Must Be Preserved ................................................ 42

3.3 How Should ESI Be Preserved? ....................................................................... 44
### TABLE OF CONTENTS
(continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3.1 Obligation to Issue a Written Legal Hold Notice</td>
<td>45</td>
</tr>
<tr>
<td>3.3.2 Elements of a Legal Hold Notice</td>
<td>45</td>
</tr>
<tr>
<td>3.3.3 Identifying and Interviewing Custodians</td>
<td>48</td>
</tr>
<tr>
<td>3.3.4 Preservation in Place vs. Preservation by Collection</td>
<td>50</td>
</tr>
<tr>
<td>3.3.5 Monitoring Compliance with a Legal Hold</td>
<td>51</td>
</tr>
<tr>
<td>3.3.6 Reissuing the Litigation Hold</td>
<td>52</td>
</tr>
<tr>
<td>3.4 What Are the Consequences for Failure to Preserve?</td>
<td>53</td>
</tr>
<tr>
<td>3.5 When Can Preservation Cease?</td>
<td>56</td>
</tr>
<tr>
<td><strong>CHAPTER 4 Requests and Scope</strong></td>
<td>57</td>
</tr>
<tr>
<td>4.1 The Rule 26 Meet and Confer</td>
<td>57</td>
</tr>
<tr>
<td>4.2 Initial Disclosures</td>
<td>63</td>
</tr>
<tr>
<td>4.3 Propounding Requests to Produce ESI</td>
<td>63</td>
</tr>
<tr>
<td>4.3.1 Define the Scope: Specify Date Ranges, Custodians, and Key Issues</td>
<td>64</td>
</tr>
<tr>
<td>4.4 Responding to Requests to Produce ESI</td>
<td>69</td>
</tr>
<tr>
<td>4.5 Interrogatories</td>
<td>73</td>
</tr>
<tr>
<td>4.6 Inspections</td>
<td>75</td>
</tr>
<tr>
<td>4.7 Requests for Admission</td>
<td>77</td>
</tr>
<tr>
<td>4.8 30(b)(6) Depositions</td>
<td>78</td>
</tr>
<tr>
<td>4.9 Subpoenas</td>
<td>80</td>
</tr>
<tr>
<td><strong>CHAPTER 5 Collection and Processing</strong></td>
<td>83</td>
</tr>
<tr>
<td>5.1 Data Collection</td>
<td>83</td>
</tr>
<tr>
<td>5.1.1 When to Collect Data</td>
<td>83</td>
</tr>
<tr>
<td>5.1.2 Collection Methods</td>
<td>84</td>
</tr>
<tr>
<td>5.1.3 Metadata</td>
<td>86</td>
</tr>
<tr>
<td>5.2 Data Processing</td>
<td>87</td>
</tr>
</tbody>
</table>
### TABLE OF CONTENTS
(continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.1 Processing</td>
<td>88</td>
</tr>
<tr>
<td>5.2.2 Filtering Techniques</td>
<td>88</td>
</tr>
<tr>
<td>5.3 Vendors and Experts</td>
<td>91</td>
</tr>
<tr>
<td>5.3.1 The eDiscovery Vendor Market</td>
<td>91</td>
</tr>
<tr>
<td>5.3.2 Vendor Selection</td>
<td>92</td>
</tr>
<tr>
<td>5.3.3 Vendor Services</td>
<td>92</td>
</tr>
<tr>
<td>5.3.4 Vendor Pricing</td>
<td>93</td>
</tr>
<tr>
<td>5.4 Special Considerations</td>
<td>94</td>
</tr>
<tr>
<td>5.4.1 International Data Protection Laws and Discovery</td>
<td>94</td>
</tr>
<tr>
<td>5.4.2 Privacy</td>
<td>100</td>
</tr>
<tr>
<td>5.4.3 Cloud Computing</td>
<td>102</td>
</tr>
<tr>
<td>5.4.4 Social Media</td>
<td>105</td>
</tr>
<tr>
<td><strong>CHAPTER 6 Analysis and Review</strong></td>
<td>111</td>
</tr>
<tr>
<td>6.1 Review Technologies</td>
<td>111</td>
</tr>
<tr>
<td>6.2 Analysis</td>
<td>111</td>
</tr>
<tr>
<td>6.3 Review</td>
<td>115</td>
</tr>
<tr>
<td>6.3.1 Pre-review Planning and Work</td>
<td>115</td>
</tr>
<tr>
<td>6.3.2 Document Review</td>
<td>116</td>
</tr>
<tr>
<td>6.3.3 Post-review Work</td>
<td>117</td>
</tr>
<tr>
<td>6.4 Technology Assisted Review (TAR)</td>
<td>117</td>
</tr>
<tr>
<td>6.4.1 TAR in Case Law</td>
<td>118</td>
</tr>
<tr>
<td>6.5 Privilege Concerns and Strategy</td>
<td>120</td>
</tr>
<tr>
<td>6.5.1 Defining the Attorney-Client Privilege and Work-Product Doctrine</td>
<td>121</td>
</tr>
<tr>
<td>6.5.2 The Federal Rules of Civil Procedure’s Approach to Privilege in the Age of eDiscovery</td>
<td>123</td>
</tr>
<tr>
<td>6.5.3 Waiver</td>
<td>124</td>
</tr>
<tr>
<td>6.5.4 Federal Rule of Evidence 502</td>
<td>126</td>
</tr>
</tbody>
</table>
TABLE OF CONTENTS
(continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.5.5 Cases Applying Rule 502(b)</td>
<td>128</td>
</tr>
<tr>
<td>6.5.6 Protective Orders and Clawback Agreements Under Rule 502(d)</td>
<td>132</td>
</tr>
<tr>
<td>6.5.7 Suggested Best Practices</td>
<td>135</td>
</tr>
<tr>
<td>6.5.8 A Special Note on Privilege Logs</td>
<td>136</td>
</tr>
<tr>
<td>6.6 Special Considerations for an Employer in Possession of an Employee's Privileged Communications</td>
<td>138</td>
</tr>
<tr>
<td><strong>CHAPTER 7 Production and Presentation</strong></td>
<td>141</td>
</tr>
<tr>
<td>7.1 Production</td>
<td>141</td>
</tr>
<tr>
<td>7.1.1 Form of Production</td>
<td>141</td>
</tr>
<tr>
<td>7.1.2 Organization of the Document Production</td>
<td>147</td>
</tr>
<tr>
<td>7.2 Presentation – Using ESI in the Courtroom</td>
<td>147</td>
</tr>
<tr>
<td>7.2.1 Admissibility Under Federal Rules of Evidence 104(a) and (b), and 901(a)</td>
<td>148</td>
</tr>
<tr>
<td>7.2.2 Relevance Under Federal Rules of Evidence 401, 105, and 402</td>
<td>149</td>
</tr>
<tr>
<td>7.2.3 Authenticity Under Federal Rules of Evidence 901 and 902</td>
<td>150</td>
</tr>
<tr>
<td>7.2.4 Hearsay Under Federal Rules of Evidence 801 to 807</td>
<td>160</td>
</tr>
<tr>
<td>7.2.5 The Original Writing (Best Evidence) Rule (Federal Rules of Evidence 1001 to 1008)</td>
<td>166</td>
</tr>
<tr>
<td>7.2.6 Probative Value vs. Prejudice Under Federal Rule of Evidence 403</td>
<td>169</td>
</tr>
<tr>
<td>7.2.7 Judicial Notice Under Federal Rule of Evidence 201</td>
<td>170</td>
</tr>
<tr>
<td><strong>CHAPTER 8 Spoliation and Electronic Discovery Sanctions</strong></td>
<td>171</td>
</tr>
<tr>
<td>8.1 The Authority to Impose Sanctions</td>
<td>172</td>
</tr>
<tr>
<td>8.2 What Is Spoliation?</td>
<td>174</td>
</tr>
<tr>
<td>8.3 Conduct Giving Rise to Spoliation Sanctions Under Rule 37(e)</td>
<td>174</td>
</tr>
<tr>
<td>8.4 Examples of Spoliation Conduct for Which Sanctions Have Been Awarded</td>
<td>180</td>
</tr>
<tr>
<td>8.5 Examples of Other Electronic Discovery Misconduct Giving Rise to Sanctions</td>
<td>182</td>
</tr>
<tr>
<td>8.6 Types of Sanctions Available</td>
<td>182</td>
</tr>
<tr>
<td>8.7 Sanctions Imposed Against Outside Counsel</td>
<td>195</td>
</tr>
</tbody>
</table>
### TABLE OF CONTENTS
(continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.8</td>
<td>The Independent Tort of Spoliation</td>
<td>200</td>
</tr>
<tr>
<td>8.9</td>
<td>Are Sanctions Inevitable?</td>
<td>203</td>
</tr>
<tr>
<td>9.1</td>
<td>Glossary of Common eDiscovery Terms</td>
<td>205</td>
</tr>
<tr>
<td>9.2</td>
<td>Petabyte, Terabyte, Gigabyte – What do these mean for eDiscovery?</td>
<td>226</td>
</tr>
<tr>
<td>9.3</td>
<td>eDiscovery Authorities</td>
<td>228</td>
</tr>
<tr>
<td>9.4</td>
<td>Overview of eDiscovery Statutes</td>
<td>274</td>
</tr>
<tr>
<td>9.5</td>
<td>Potential Sources of Information</td>
<td>299</td>
</tr>
<tr>
<td>9.6</td>
<td>Morgan Lewis eData Practice</td>
<td>301</td>
</tr>
</tbody>
</table>

### CHAPTER 9 Appendices

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>205</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1</td>
<td>Glossary of Common eDiscovery Terms</td>
<td>205</td>
</tr>
<tr>
<td>9.2</td>
<td>Petabyte, Terabyte, Gigabyte – What do these mean for eDiscovery?</td>
<td>226</td>
</tr>
<tr>
<td>9.3</td>
<td>eDiscovery Authorities</td>
<td>228</td>
</tr>
<tr>
<td>9.4</td>
<td>Overview of eDiscovery Statutes</td>
<td>274</td>
</tr>
<tr>
<td>9.5</td>
<td>Potential Sources of Information</td>
<td>299</td>
</tr>
<tr>
<td>9.6</td>
<td>Morgan Lewis eData Practice</td>
<td>301</td>
</tr>
</tbody>
</table>
Good information governance has become irreplaceable in the age of eDiscovery. Although much of the recent focus, and the angst, related to eDiscovery has centered on the extraordinary volumes of data that drive up litigation expense and can lead to eye-popping verdicts resulting from missteps and omissions, organizations can do much to reduce the cost and risks of eDiscovery with effective information management.

Information governance is a set of interrelated disciplines that together provide a framework of policies, processes, and roles that enable an organization to organize, secure, maintain, retrieve, and dispose of information in a manner that meets business goals while also satisfying legal and regulatory obligations. It considers the needs of the business, as well as the systems and processes necessary to support the business while addressing every stage in the information life cycle—from creation and security through retention and disposition. Simply put, information governance is a holistic, integrated approach to leveraging the information that drives today’s businesses.

Effective information governance also presents the first and best opportunity for an organization to gain some control over the eDiscovery process. Organizations can substantially limit risks and achieve cost efficiencies with a robust information governance program that includes an eDiscovery plan.

Among other benefits, an information governance program can:

- Reduce storage costs
- Reduce litigation risk
- Reduce the cost of discovery
- Enforce corporate compliance
- Ensure sound cybersecurity and privacy protection
- Provide business continuity
- Ease organization, storage, and retrieval of business records
- Defensibly dispose of expired records
In addition, a comprehensive, consistently enforced program becomes a defense to claims of spoliation when failure to produce records in litigation is the result of such a program.¹

Despite these obvious benefits, few companies have robust information governance programs that address the retention, storage, and disposal of electronically stored information (ESI) or aim to leverage business information as an asset.² Moreover, most companies fail to address newer technologies and forms of ESI.³ As a result, most organizations are likely to be massively over-retaining records for no legitimate business or legal reason.⁴ Research indicates that 69% of the information retained by companies should be destroyed but is not.⁵ Given the volume and risk involved, information governance and, in particular, record retention and eDiscovery are worthy investments of time and resources that can yield a significant return.

Awareness of the sheer volume and contents of information that have been developed and stored over time makes it clear that the information needs to be managed effectively before litigation or a response to a regulatory inquiry or subpoena. Planning and implementing an information governance program not only manages liability and risk but can also identify hidden assets: knowing what you have, where it is kept, how it is—and is not—being used, and how it might be used are all benefits of having a functional governance program.⁶

Identifying and accessing information using interdisciplinary teams and processes enhance retrieval for eDiscovery and other purposes and also increase opportunities to share cross-business ideas, enhance quality and service delivery, strengthen data security, and identify gaps in knowledge and opportunities for improvement and growth.⁷ A framework for determining the value of information assets starts with mapping the sources of asset information, identifying the location and dimension of the asset, calculating the net potential value of the asset, and computing the option value of assets being left “on the table” by the organization, as a result of either perceptions of risk or missed opportunities.⁸

---

1. See Arthur Andersen LLP v. United States, 544 U.S. 696 (2005); Park v. City of Chicago, 297 F.3d 606 (7th Cir. 2002); Lewy v. Remington Arms Co., 836 F.2d 1104 (8th Cir. 1988); cf. Testa v. Wal-Mart Stores, Inc., 144 F.3d 173 (1st Cir. 1998).


5. See Derek Gascon, The Risk of Keeping Too Much Data, Risk Mgmt. (Dec. 1, 2013) (citing the Compliance Governance & Oversight Council research that “typically only 1% of corporate information is on litigation hold, 5% is in records retention, and 25% has current business value. This means that as much as 69% of all the data organizations collect has no business, legal or regulatory value at all.”).


7. Id.

8. Id.
2.1 The Basic Questions

Record retention policies and procedures are essential to information governance. Developing comprehensive and defensible programs in a complex environment of federal and state laws that govern the management of business records provides a structure in which information assets can be managed to ensure legal compliance, promote consistency, reduce discovery and storage costs, and mitigate the risks associated with over retaining or under retaining your records. Identifying applicable legal requirements for retention and destruction of records, performing comprehensive assessments of where information is stored and how to retrieve and produce the information, and developing a plan for litigation are essential steps for managing litigation risk and supporting an effective Enterprise Risk Management (ERM) program.

2.1.1 The Legal and Regulatory Landscape

A critical step in drafting a retention policy and schedule is identifying the applicable legal requirements concerning the retention and destruction of information. An organization must consider the externally mandated laws and regulations that govern it (e.g., from the IRS, SEC, DOD, DOL/EOC, EPA), as well as its duties to preserve data potentially relevant to actual or reasonably anticipated litigation.9

<table>
<thead>
<tr>
<th>FAQs</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is a retention policy?</td>
</tr>
<tr>
<td>A retention policy is a document describing the principles and practices implemented to manage documents and data that constitute an organization’s “business records.”</td>
</tr>
</tbody>
</table>

| What is a retention schedule?    |
| A retention schedule is a taxonomy listing the “business records” of the organization and the length of time the organization will store each record type. |

| Why not use an “off-the-shelf” policy or schedule? |
| Organizations differ widely in the “business records” they maintain and in the legal, regulatory, industry, and business retention obligations with which they must comply. A policy and schedule should be custom designed for each specific organization. |

For organizations with international operations or data, determining all applicable legal requirements can be very complicated.

For example, Article 8 of the Charter of Fundamental Rights of the European Union (2000/C364/01) recognizes that every person has a right to the protection of personal data and that such data must be processed fairly and for specified purposes, and on the basis of the consent of the person or some other

9. See, e.g., Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC, 685 F. Supp. 2d 456, 466 (S.D.N.Y. 2010) (once a party reasonably anticipates litigation, it must suspend its routine retention/destruction policy and put in place litigation hold to ensure preservation of relevant documents); Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 216 (S.D.N.Y. 2003) (“Zubulake IV”) (obligation to preserve arises when party knows or should have known that evidence is relevant to current or anticipated litigation).
legitimate lawful basis. This right includes the fundamental right to access personal data and to correct any mistakes within that data.

The legislation protecting individuals’ rights in relation to personal data is mostly contained within Directive 95/46/EC on Data Protection, which seeks to harmonize the applicable national legislations of the member states. Although this legislation neglects to address such developing technologies as social networking and cloud computing, the European Commission recently unveiled a draft European General Data Protection Regulation (GDPR) that will supersede the Data Protection Directive and unify the data protection laws within the European Union by early 2018.

In the People’s Republic of China, on the other hand, there is limited regulation of document retention in place, but it is generally understood that the civil law principle protecting the right to privacy also applies in relation to the protection of personal data.

**Monitoring and Compliance: Essential Components of a Retention Program**

Beyond the strict legal requirements, a reasonable retention program serves the operational needs of an organization. A retention schedule should identify and prescribe time periods for the retention of information as appropriate for an organization’s information storage, access, and retention needs, and its legal responsibilities. Such a schedule serves a legitimate business purpose, but is not designed to eliminate potential “smoking guns.”

The mere existence of a written policy will not establish that document destruction was justified. Without a sound monitoring and compliance program, an information management policy may be criticized as eliminating only “bad” documents.

An organization focused on eliminating “bad” documents not only risks accusations of bad faith (or worse), but also fails to recognize the value of contextual documents in mitigating the so-called “bad” documents and potentially exonerating the organization from allegations of misconduct or wrongdoing.

The consequences for ill-conceived retention programs that merely serve as vehicles to “cleanse” files in advance of anticipated litigation or investigation can be severe. For example, in civil litigation, retention programs that focus on eliminating “bad” documents may be criticized as illegitimate “document destruction” policies that may result in severe sanctions, including default judgment, as shown in the following decisions:

---

10. See *Levy*, 836 F.2d at 1112 (part three of a three-part test to evaluate the reasonableness of a defendant’s retention program addresses whether the program was instituted in bad faith).

11. See *Carlucci v. Piper Aircraft Corp.*, 102 F.R.D. 472, 485 (S.D. Fla. 1984) (failure to implement the retention policy in a consistent manner was a significant factor in finding that the destruction of certain evidence relevant to legal proceedings could not be explained or excused as compliance with the policy).

12. See *Arthur Andersen LLP v. United States*, 374 F.3d 281, 297 (5th Cir. 2004) (“There is nothing improper about following a document retention policy when there is no threat of an official investigation, even though one purpose of such a policy may be to withhold documents from unknown, future litigation. An organization’s sudden instruction to institute or energize a lazy document retention policy when it sees the investigators around the corner, on the other hand, is more easily viewed as improper.”), *rev’d on other grounds*, 544 U.S. 696 (2005).
A focus on concealment and damage control, as opposed to targeted retention based on operational, legal, or institutional value, may even result in criminal penalties. For example, sections 802 and 1102 of the Sarbanes-Oxley Act of 2002 provide for fines and/or up to 20 years’ imprisonment for destroying or concealing documents or other evidence with the intent to impair their availability for use in a proceeding or with the intent to impede, obstruct, or influence federal investigations or bankruptcy proceedings.

2.1.2 Data Assessment

The data assessment process is designed to catalog and assess the company’s electronic data management systems. A 2009 survey of business use of email found that a third of organizations have no policy to deal with legal discovery and 40% would likely have to search backup tapes to find emails that might be relevant to litigation. The survey also found that 84% would have no way to justify why emails of a certain age or type would have been deleted, only 19% have the facility to move important emails into a document management system or a dedicated email system, and 45% are still filing their important emails in personal Outlook® folders.\(^{13}\) While email management practices have certainly improved since then, many organizations migrating to the cloud are only now confronting lax policy enforcement and massive volumes of undermanaged email.

The best time to complete a data assessment is before litigation strikes, when the organization has the luxury of time to complete a comprehensive review of its data inventory, information, policies, and eDiscovery response strategy. (For information on this, see section 2.2.4, eDiscovery Readiness.) Even if undertaken at the outset of active litigation, a data assessment is an essential tool for managing all aspects of the discovery process.

---

13. 2009 AIIM Email Management: The Good, the Bad, and the Ugly, available from the authors at www.aiim.org.
FAQs

What is a data assessment?

A data assessment is a gap analysis and assessment of the client’s eDiscovery management systems, including scrutiny of accessible and archived storage systems and retention practices and policies.

A data assessment should include the following:

- Identification of data sources most likely to contain responsive information in an eDiscovery context.
- Determination of how data is stored internally and by cloud providers or other third-party storage providers.
- Determination of how data is backed up, archived, or otherwise preserved, and for what length of time, including rotation schedules.
- Determination of which data sources are “readily accessible” and which ones are not.
- Identification of historical operating systems and applications.
- Identification of search capabilities of the various data sources.
- Identification of how and whether “former employee” data is managed, maintained, and preserved.
- Estimated cost of retrieving and accessing ESI.
- Assessment of the client’s policies and procedures for electronic data use, management, and retention.

Depending on the nature of the matter, it may be preferable to work with the individual owners of the data systems to identify all ESI sources and forms. It may also be necessary to follow up with your cloud provider to determine how data is being retained, protected, backed up, or preserved in the event of litigation.

2.2 Programs and Policies

2.2.1 Retention Programs

A retention program consists of a retention policy and schedule, and addresses retention and disposition of information in all forms: creation and storage of electronic documents and information; email on desktops, laptops, instant messaging programs, and iPhone and other smart phones, tablets, and similar devices; websites; data recorders; backup tapes; servers; audio and video recordings; and paper and other physical manifestations of information. The objectives of any information retention program should be twofold:

- Reduce the overall cost of retention and storage by disposing of those records that have outlived their legal, regulatory, and business use; and
- Retain information necessary to meet any legal and regulatory requirements of the business, and the continued operation and enhanced profitability of the business.
Implied within these objectives is the fundamental principle of eDiscovery—that an organization should “know where its stuff is.” If an organization has a good handle on the location, source, and content of its information, it should be well equipped to respond to requests for ESI in an efficient and defensible manner.

Development of a retention program is the first and, to some degree, most important step an organization can take in developing an effective eDiscovery response mechanism. A robust retention policy and schedule that are carefully crafted, effectively implemented, and consistently applied will reduce the volume of information maintained by the organization.

Once an organization has researched its retention obligations and mapped its records taxonomy, it can then assess its current recordkeeping practices and begin to identify the technical and human resources needed to enhance its ability to store, access, and dispose of its records effectively and defensibly.

It is widely agreed that retention policies and schedules should be simple but comprehensive. They should address all types of documents, both physical and electronic (including email, data files, voicemail, etc.). The ideal retention schedule provides for the shortest retention periods legally and operationally possible, and a cutting-edge policy is automated to take the guesswork and compliance out of employees’ hands.

An effective retention program should meet the following criteria:

- Meets business needs and legal obligations
- Is comprehensive, yet simple
- Addresses both electronic and paper data
- Clearly states rationale for policy
- Includes retention/disposition schedules
- Includes an exception for legal holds
- Is widely communicated
- Is easily accessible
- Is simple to follow

Keep the following in mind during the creation of your retention program:

- Designate a gatekeeper or information-management team that understands the company’s IT infrastructure and capabilities
- Identify the records groups: Tax, Human Resources, Finance, Accounting, Sales and Marketing, Corporate, etc.
- Inventory business records by interviewing representatives of each business function and/or business unit
- Remember that an ignored or inconsistently applied policy is worse than no policy at all
- Develop a comprehensive process for auditing and promoting compliance within the company
Employee training and education is the key to implementation, and should include the following:

- Litigation primer
- Best practices
- Retention program implementation
- Importance of program
- Distinction between “business records” and “records of transitory value”
- How to store and dispose of business records in accordance with the program

Potential consequences of failure to properly retain records include the following:

- Civil or criminal penalties, including adverse inference instructions
- Penalties under Sarbanes-Oxley Act of 2002
- Infractions under Title 18 – Obstruction of Justice

**Retention Policy**

A retention policy explains the scope of the retention program, its policies and procedures, personnel responsibilities, and applicability of the policy. A sound retention policy will clearly and unambiguously articulate the following:

- Reasons for the policy
- Requirements of the policy (e.g., clearly defined categories of information to be retained, retention requirements consisting of a retention schedule, and procedures for retention and disposition)
- The parties responsible for establishing program controls and providing active, ongoing management
- Safeguards to suspend the retention policy and disposition schedule in the case of anticipated, pending, or active litigation or government investigation (Legal Hold Process)
- The organizational commitment to compliance with the policy

**Retention Schedule: The Record Taxonomy**

The retention schedule sets forth a concise inventory of the information to be retained and the retention periods for retained information in order to reduce risk and costs associated with information retention.

In order to identify the universe of information to be included in a schedule, an organization should understand the fundamental intent of the types of information it generates and receives so that it can
establish a relevant schedule for both the information that must be retained and the information that should be disposed.\textsuperscript{14}

Typically, organizations opt to establish varying retention periods that will satisfy legal requirements concerning each category of information, while at the same time trying to maintain a simplified process so that the program can be implemented without confusion. Establishing logically related but workable record groups according to the information’s characteristics, such as functionality or the regulatory authority governing retention, appears to be the best practice.

The best means to establish these records groups is to understand why and when an organization’s employees create information in the course of business and what type of information they create, i.e., a record taxonomy. This taxonomy not only aids in establishing a proper retention schedule for all information, but also identifies inconsistencies in practice in developing information (both hard copy and electronic versions)—which can also be used in addressing information management system issues and in training employees to minimize practices that can result in significant variations in how business information is created.

By understanding what information is created within the various business functional areas of the organization, decisions can then be made as to the type of retention schedule it wishes to implement, whether general or specific:

- **General schedule** (“big bucket“): All documents within each records group are subject to the same retention period (e.g., all organization information created in the course of business relating to tax issues will be disposed of within seven years of its creation), with different retention periods applying to different types of information, as appropriate. The retention period for each group should reflect the longest retention period applicable to a particular type of document within that group. As a result, this type of schedule is generally shorter and more streamlined than a schedule where each information type is listed separately (see “Specific schedule” below), but the trade-off is longer retention periods.

- **Specific schedule**: Retention periods are tailored to meet the legal and operational retention requirements of each different type of information generated for business use, and each such period is listed separately. This system is useful for companies that prefer a more granular set of retention periods in exchange for shorter retention periods.

\textsuperscript{14} Best practice also necessitates that an organization review its litigation activity in recent years, and any action involving regulatory agencies that oversee its business, to ensure that it understands the compliance obligations associated with those matters.
Practice Pointer: Disposition of ESI

- Disposition is an acceptable stage in the information life cycle; an organization may delete electronic information when there is no continuing value or need to retain it.

- Systematic deletion of electronic information is not synonymous with evidence spoliation.

- In the absence of a legal requirement to the contrary, organizations may adopt programs that routinely delete certain recorded communications, such as email, instant messaging, text messaging, and voicemail.

- In the absence of a legal requirement to the contrary, organizations may recycle or destroy hardware or media that contain data retained for business-continuation or disaster-recovery purposes.

- In the absence of a legal requirement to the contrary, organizations may systematically destroy residual, shadowed, or deleted data.

With an eye toward simplification, many companies opt for the general retention schedule, taking a “big bucket” approach by consolidating multiple types of information into broad categories as opposed to assigning different retention periods to each different information type. The current trend is toward consolidation: categorizing and prioritizing retention by activity and function as opposed to classification systems with multiple categories and increased complexity. However, after analyzing its records inventory, each organization must determine for itself which system will work most effectively while still complying with the relevant legal requirements.

2.2.2 ESI Policies

In addition to the retention policy and schedule, every organization should create eData policies related to the use of the organization’s information technology. Some fairly typical IT policies include email and acceptable-use policies.

Email Policies

Few retention policies drafted prior to the year 2000 address the subject of email. Yet email presents the greatest management challenge, primarily due to the sheer volume of emails generated each day in U.S. businesses. Email should be subject to an organization’s retention program just as Excel spreadsheets or PowerPoint presentations are, but there are additional considerations for how email should be maintained within the email system, such as regulatory requirements, system requirements or limitations, and data privacy when dealing with non-U.S. employees or storage. See Chapter 5, Collection and Processing.

Many options exist for email policies, including the following:

- **Cap and purge**: Puts a cap on the size of each user’s mailbox and purges emails that have reached a certain age (typically 60 to 90 days).

- **Cap and archive**: Puts a cap on the size of each user’s mailbox and allows users to create local archives of emails they wish to save.
• **All-in archive**: All incoming and outgoing email is stored indefinitely in an archive.

• **Selective rule archive**: Captures all email and uses sophisticated searches to automatically identify and classify business records, subject to retention obligations.

• **Selective declared archive**: Requires users to classify each email and store it in a designated archive location.

• **Role-based archive**: Captures email and applies retention periods based on the job classification of the sender or recipient.

• **Unlimited email server storage**: Saves all email on the server indefinitely.

Each of these options has significant pros and cons related to cost, likelihood of compliance, and ease of access. No option is a perfect solution; the efficacy of each differs among organizations and their particular needs. A careful assessment of an organization’s corporate structure, IT infrastructure, retention program, and litigation portfolio is necessary to select the best approach.

**Acceptable-Use Policies**

Acceptable-use policies are codes of conduct that describe both acceptable use of an organization’s computers and prohibited activities. Most of these policies relate to acceptable use of email and the Internet. Such policies have become increasingly necessary in recent years, due to the following trends in Internet use:

• 70% of Internet porn traffic occurs between the hours of 9 a.m. and 5 p.m.

• 75% of large organizations suffer staff-related data breaches.\(^\text{15}\) 27% of Fortune 500 companies have drawn harassment claims stemming from employees’ misuse of email and the Internet.\(^\text{16}\)

• Workers waste 60 to 80% of their time on the internet “cyberslacking”—surfing the Web for personal reasons or no reason at all.\(^\text{17}\)

A typical acceptable-use policy should include the following:

• Establish that all computers and related hardware (e.g., organization-provided PDAs, cell phones, tablets, and portable media), along with the content on those devices, are the property of the organization.

• Clearly state that such devices are provided to employees for business purposes only and should not be used for personal reasons.

---


\(^\text{17}\) See Joseph Ugrin, All play, no work: Policy, enforcement may stop employees from wasting time online at work, researcher finds, K-State News (Jan. 31, 2013), https://www.k-state.edu/media/newsreleases/jan13/cyberloaf13113.html (last visited May 16, 2017).
• State in unequivocal terms that the organization is entitled to and does monitor Internet and email usage. (Here the organization must “put its money where its mouth is,” and engage in some sort of compliance monitoring in order for this policy to afford the organization protection from liability.)

• Describe prohibited activities, including, but not limited to, solicitation; harassment; disclosure of confidential information; illegal activities; the making of defamatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, obscene, or otherwise disruptive statements; political activity; and any activity likely to disrupt business operations, including downloading prohibited content or virus-infected materials.

• Prohibit downloading software applications, including instant messengers, music-sharing tools, and other peer-to-peer applications.

• Describe the repercussions for failure to comply.

As with retention policies, an acceptable-use policy is only as good as an organization’s wherewithal to train its workforce and monitor compliance. Implementation that emphasizes consistent monitoring and training during the rollout of the policy is critical.

Other Technology Policies

Many companies and individuals are tech savvy, or so-called “über users.” When this is the case, acceptable-use policies should be expanded to include social networking, instant messaging (IM), VoIP (Internet-based telephone systems), blogging, text messaging, and so forth to circumscribe use as appropriate to the needs of the organization. As illustrated by a case involving a supervisor’s review of an employee’s text messages, an acceptable-use policy will overcome an employee’s expectation of privacy.

A Note on Instant and Text Messaging

Researchers have found that IM has been in use in more than 90% of companies for some time. Yet, of those companies, many report that their IM activity is not controlled by the organization, but is accessed by individual employees from Internet service providers or public apps, such as Snapchat, Google Chat, WhatsApp, and Facebook. Moreover, retention becomes even harder for corporations as 24% of individuals use messaging apps that automatically delete sent messages. Similarly, while 80 percent of employees use text messaging for business, text messages, even if generated on an organization-issued

---

18. See Stengart v. Loving Care Agency, Inc., 990 A. 2d 650 (N.J. 2010) (Employee's communications with her attorney were privileged even though they were sent using a company computer where, among other considerations, the court found the employee's communications policy ambiguous because it allowed for occasional personal use of email and thus did not clearly establish that there was no reasonable expectation of privacy).

19. See City of Ontario, Cal., et al. v. Quon, et al., 130 S. Ct. 2619 (2010) (employer’s search of employee’s text messages on work-issued pager did not violate employee’s Fourth Amendment right to privacy where employer had policy regarding computer usage, Internet, and email that warned that all network activity might be monitored and that users had no expectation of privacy or confidentiality when emailing or using network resources).


22. See Nathan Eddy, BusinessTextingGrows More Widespread, eWeek (May 22, 2015), at http://www.eweek.com/small-
smartphone, are not retained by the organization, if they are retained at all. Yet it is clear from a
developing body of case law and commentary that IM and text messages, like email, constitute
discoverable ESI. Organizations must therefore assess the use and retention obligations of IM and text
messages, and implement policies to establish greater control over these communication tools.

The key decision here for businesses: to IM/text or not to IM/text? If an organization concludes that IM
and text messaging enhance the productivity of its business, then it must enact policies and technologies
to manage and control their use. If these technologies do not enhance business operations, then the
organization must enact policies and technologies to limit or prohibit their use for business purposes. Both
options remain common in today’s business environment.

### 2.2.3 Technological Solutions

A host of technology solutions are available to ease implementation and compliance with a retention
program. Given the volume of data generated and received by organizations in the ordinary course of
business, technology tools to manage the flow, organization, and retention of eData are mission critical.
Among the tools organizations should consider are:

1. **Email management solutions**: These tools capture, regulate, and archive email traffic
   according to rules defined by the organization to meet its operational and compliance needs.
   Many such tools come with robust search and retrieval capabilities, single-instance archiving,
   and legal hold and eDiscovery functionality.

2. **eData management solutions**: These tools apply retention principles to user-generated
   files and offer a single archive for records storage and retrieval. Such tools offer an effective
   alternative to uncontrolled user data management, such as local archiving and subject-matter
   drives.

3. **Legal hold management**: These tools manage the legal hold process, including distribution
   of legal hold notices and compliance tracking.

4. **eDiscovery management**: An array of tools are entering the market that are designed to
   assist organizations in searching, harvesting, analyzing, culling, processing, and hosting data
   subject to eDiscovery.

The selection of technology solutions should first and foremost be a partnership between the
organization’s IT and legal teams. This multidimensional team should consider many factors, including the
size of the organization’s litigation portfolio, data volume, IT infrastructure, and other resources.
Ultimately, to support the policies and protocols that the organization establishes for retention, ESI, and

---

23. According to research firm Radicati, the total number of business and consumer emails sent and received per day in
    2017 will reach 269 billion, expanding to 319.6 billion per day by the end of 2021. See The Radicati Group, Inc., *Email
2.2.4 eDiscovery Readiness

A thoughtful, repeatable eDiscovery response plan (i.e., a litigation-readiness plan) works hand in hand with a retention program. Such a plan identifies the processes and resources the organization will deploy to meet its preservation and discovery obligations when faced with threatened or actual litigation, a government inquiry, or a subpoena. An eDiscovery readiness plan may have many components, including data inventories, response protocols, forms, and templates. All are designed to meet enhanced discovery obligations imposed by the amended Federal Rules of Civil Procedure, state rules, and a growing body of case law. The plan should be designed to identify and preserve all potentially relevant sources of eData as well as determine how the organization will ultimately collect and produce that data.

A critical function of any effective information governance program is the orderly suspension of ordinary-course disposal when certain information must be preserved due to anticipated or pending litigation or government inquiry. Developing a litigation-readiness plan expands upon the exception described in a retention policy and positions an organization to meet the enhanced obligations imposed by the Federal Rules of Civil Procedure.

An eDiscovery readiness plan enables an organization to do the following:

- Effectively and efficiently respond to requests for ESI
- Avoid duplication of effort in multiple cases
- Promote the defensibility of the process
- Minimize business disruptions and related expenses
- Reduce the risk of inconsistent responses from case to case

The eDiscovery readiness plan identifies milestones, roles, and responsibilities in the litigation-response process. The plan further establishes standard protocols for data gathering, collection, preservation, and processing, in addition to data-production requirements. Matter classification guidelines identifying resources that the organization will deploy in defined classes of cases are an integral part of the plan. The plan also helps the organization issue legal hold notices, Rule 26(a) Initial Disclosures, and Form 35 Discovery Plans that are consistent across federal and state litigation, as well as in response to requests from federal and state regulatory agencies.

2.2.5 Training and Implementation

An essential component of any information management program is the implementation phase. After the program is developed, the focus should turn to implementation, which involves (a) preparation of training materials for implementation, enforcement, compliance, and auditing; (b) training of an internal records management committee and/or manager; (c) internal publication of the retention program and training of organization personnel; and (d) supervision and documentation of the first round of retention program enforcement.
In addition, organizations should investigate, analyze, pilot, and select technological solutions to automate and facilitate the information management process if technology will be deployed to enhance implementation and compliance.

2.2.6 Audit

Given the volume of information generated by an organization on a regular basis, ever-evolving legal requirements for retention and production, and the changing business needs of an organization, administering a defensible retention program requires regular management.

Auditing and compliance are fundamental elements of a retention program. Courts examine these elements to determine whether a retention program is reasonably designed to meet the legitimate legal and business needs of the organization, or is merely a haphazard program that eliminates documents and data relevant to pending or anticipated litigation. In addition to providing evidence of systemic monitoring and compliance with the retention program, an annual review or audit gives an organization the opportunity to leverage informational assets by identifying the potential for information sharing, gap analysis, and cost efficiencies in its remote business functional areas.

Many options exist for conducting an effective audit. Two options, a full audit and a selective audit, are described in this section.

Full Audit

Depending on the current state of a client’s retention program, records inventory, and compliance history, a full audit of all records of a significant sampling of organization personnel may be warranted. A full audit would entail interviews and inspections of employees across all locations and business functional areas. A full audit is a sensible approach when an organization has not previously implemented or enforced a retention program, does not have internal resources to implement a new retention schedule for historical records, has “inherited” information from predecessor organizations, and/or has a volume of historical information that presents additional challenges.

Selective Audit

The second option is to complete a selective audit by, first using online questionnaires and certifications, and then selecting for interviews and inspections 1% to 5% of employees across the organization’s locations and functional areas. A selective audit is a sensible approach for an organization that has historically engaged in some manner of information management and/or retains a manageable volume of records.

2.2.7 Refreshing Retention Schedules

Organizations are also encouraged to conduct a yearly “refresh” of the retention schedule to ensure that scheduled retention obligations are current with legal and regulatory requirements.
ACKNOWLEDGMENTS

The eData practice at Morgan Lewis was founded in 2004, just two years before the Federal Rules of Civil Procedure (Federal Rules) were amended to accommodate the growing role of electronically stored information in the discovery process.

Even before eData and the amendments to the Federal Rules, our lawyers were among the few in our profession focused on this extraordinarily challenging practice area. And as this area of the law continues to grow and evolve, so has the eData practice, which has matured into a global practice group comprising more than 100 lawyers, 50 technologists, five dedicated discovery management centers, two data centers, and an offshore review team.

When we issued the initial Deskbook, it was our first attempt to gather the considerable knowledge and experience of the eData team and summarize it in a volume that would be useful to our colleagues and clients.

The second edition resulted in a substantial reorganization, following more closely the Electronic Discovery Reference Model (EDRM), as well as a comprehensive update to capture changes in the law and the evolution of this field. This area of the law continues to evolve, leading to this third edition. Exciting changes have occurred in the recent past including the 2015 Amendments to the Federal Rules and the rapidly evolving changes to the European Data Protection Laws and related obligations to collect data outside the United States. The third edition adds considerations and guidance related to information governance, social media and Data Privacy in keeping with recent and ongoing legal and technical developments and trends.

This eData Deskbook – Third Edition captures the best practices, practical advice, and experience of its contributors, to whom special thanks and acknowledgment must be given: Jennifer Mott Williams, Tara Lawler, and Lorraine Casto.

To our clients and prospective clients, we hope this eData Deskbook proves useful to you, and we look forward to working with you.

Tess Blair
Editor
TABLE OF CONTENTS

CHAPTER 1 Introduction to eDiscovery ................................................................. 1

1.1 The World of eDiscovery ................................................................................. 1

1.2 Legal Overview ............................................................................................ 2

1.2.1 The 2015 Amendments to the Federal Rules of Civil Procedure ........... 2

1.3 Ethical Implications of eDiscovery ............................................................... 6

1.3.1 The ABA Model Rules of Professional Conduct .................................. 6

1.4 The Electronic Discovery Reference Model ................................................. 9

CHAPTER 2 Information Governance ................................................................. 13

2.1 The Basic Questions .................................................................................... 15

2.1.1 The Legal and Regulatory Landscape .................................................. 15

2.1.2 Data Assessment ................................................................................. 17

2.2 Programs and Policies ................................................................................ 18

2.2.1 Retention Programs ........................................................................... 18

2.2.2 ESI Policies ...................................................................................... 22

2.2.3 Technological Solutions ...................................................................... 25

2.2.4 eDiscovery Readiness ......................................................................... 26

2.2.5 Training and Implementation ............................................................... 26

2.2.6 Audit ................................................................................................. 27

2.2.7 Refreshing Retention Schedules .......................................................... 27

CHAPTER 3 Identification and Preservation ...................................................... 29

3.1 When Does a Duty to Preserve Arise? ......................................................... 29

3.2 What Must Be Preserved? ......................................................................... 33

3.2.1 Guidance from the Federal Rules ....................................................... 33

3.2.2 “Electronically Stored Information” and Its Potential Sources ............ 34

3.2.3 Possession, Custody, or Control ......................................................... 38

3.2.4 Limitations on What Must Be Preserved ........................................... 42

3.3 How Should ESI Be Preserved? ................................................................. 44
TABLE OF CONTENTS
(continued)

3.3.1 Obligation to Issue a Written Legal Hold Notice ....................................... 45
3.3.2 Elements of a Legal Hold Notice................................................................. 45
3.3.3 Identifying and Interviewing Custodians .................................................. 48
3.3.4 Preservation in Place vs. Preservation by Collection .................................. 50
3.3.5 Monitoring Compliance with a Legal Hold ................................................ 51
3.3.6 Reissuing the Litigation Hold ................................................................... 52
3.4 What Are the Consequences for Failure to Preserve? ............................................ 53
3.5 When Can Preservation Cease? ........................................................................... 56

CHAPTER 4 Requests and Scope ...................................................................................... 57
4.1 The Rule 26 Meet and Confer ............................................................................. 57
4.2 Initial Disclosures ............................................................................................... 63
4.3 Propounding Requests to Produce ESI ................................................................. 63
4.3.1 Define the Scope: Specify Date Ranges, Custodians, and Key Issues ......... 64
4.4 Responding to Requests to Produce ESI .............................................................. 69
4.5 Interrogatories ................................................................................................... 73
4.6 Inspections ........................................................................................................ 75
4.7 Requests for Admission ...................................................................................... 77
4.8 30(b)(6) Depositions .......................................................................................... 78
4.9 Subpoenas ........................................................................................................ 80

CHAPTER 5 Collection and Processing ............................................................................. 83
5.1 Data Collection .................................................................................................. 83
5.1.1 When to Collect Data ............................................................................. 83
5.1.2 Collection Methods ................................................................................. 84
5.1.3 Metadata ............................................................................................... 86
5.2 Data Processing ................................................................................................ 87
### TABLE OF CONTENTS

(continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.1</td>
<td>Processing</td>
<td>88</td>
</tr>
<tr>
<td>5.2.2</td>
<td>Filtering Techniques</td>
<td>88</td>
</tr>
<tr>
<td>5.3</td>
<td>Vendors and Experts</td>
<td>91</td>
</tr>
<tr>
<td>5.3.1</td>
<td>The eDiscovery Vendor Market</td>
<td>91</td>
</tr>
<tr>
<td>5.3.2</td>
<td>Vendor Selection</td>
<td>92</td>
</tr>
<tr>
<td>5.3.3</td>
<td>Vendor Services</td>
<td>92</td>
</tr>
<tr>
<td>5.3.4</td>
<td>Vendor Pricing</td>
<td>93</td>
</tr>
<tr>
<td>5.4</td>
<td>Special Considerations</td>
<td>94</td>
</tr>
<tr>
<td>5.4.1</td>
<td>International Data Protection Laws and Discovery</td>
<td>94</td>
</tr>
<tr>
<td>5.4.2</td>
<td>Privacy</td>
<td>100</td>
</tr>
<tr>
<td>5.4.3</td>
<td>Cloud Computing</td>
<td>102</td>
</tr>
<tr>
<td>5.4.4</td>
<td>Social Media</td>
<td>105</td>
</tr>
<tr>
<td>6.1</td>
<td>Review Technologies</td>
<td>111</td>
</tr>
<tr>
<td>6.2</td>
<td>Analysis</td>
<td>111</td>
</tr>
<tr>
<td>6.3</td>
<td>Review</td>
<td>115</td>
</tr>
<tr>
<td>6.3.1</td>
<td>Pre-review Planning and Work</td>
<td>115</td>
</tr>
<tr>
<td>6.3.2</td>
<td>Document Review</td>
<td>116</td>
</tr>
<tr>
<td>6.3.3</td>
<td>Post-review Work</td>
<td>117</td>
</tr>
<tr>
<td>6.4</td>
<td>Technology Assisted Review (TAR)</td>
<td>117</td>
</tr>
<tr>
<td>6.4.1</td>
<td>TAR in Case Law</td>
<td>118</td>
</tr>
<tr>
<td>6.5</td>
<td>Privilege Concerns and Strategy</td>
<td>120</td>
</tr>
<tr>
<td>6.5.1</td>
<td>Defining the Attorney-Client Privilege and Work-Product Doctrine</td>
<td>121</td>
</tr>
<tr>
<td>6.5.2</td>
<td>The Federal Rules of Civil Procedure's Approach to Privilege in the Age of eDiscovery</td>
<td>123</td>
</tr>
<tr>
<td>6.5.3</td>
<td>Waiver</td>
<td>124</td>
</tr>
<tr>
<td>6.5.4</td>
<td>Federal Rule of Evidence 502</td>
<td>126</td>
</tr>
</tbody>
</table>
## TABLE OF CONTENTS

(continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.5.5 Cases Applying Rule 502(b)</td>
<td>128</td>
</tr>
<tr>
<td>6.5.6 Protective Orders and Clawback Agreements Under Rule 502(d)</td>
<td>132</td>
</tr>
<tr>
<td>6.5.7 Suggested Best Practices</td>
<td>135</td>
</tr>
<tr>
<td>6.5.8 A Special Note on Privilege Logs</td>
<td>136</td>
</tr>
<tr>
<td>6.6 Special Considerations for an Employer in Possession of an Employee's Privileged Communications</td>
<td>138</td>
</tr>
<tr>
<td><strong>CHAPTER 7 Production and Presentation</strong></td>
<td>141</td>
</tr>
<tr>
<td>7.1 Production</td>
<td>141</td>
</tr>
<tr>
<td>7.1.1 Form of Production</td>
<td>141</td>
</tr>
<tr>
<td>7.1.2 Organization of the Document Production</td>
<td>147</td>
</tr>
<tr>
<td>7.2 Presentation – Using ESI in the Courtroom</td>
<td>147</td>
</tr>
<tr>
<td>7.2.1 Admissibility Under Federal Rules of Evidence 104(a) and (b), and 901(a)</td>
<td>148</td>
</tr>
<tr>
<td>7.2.2 Relevance Under Federal Rules of Evidence 401, 105, and 402</td>
<td>149</td>
</tr>
<tr>
<td>7.2.3 Authenticity Under Federal Rules of Evidence 901 and 902</td>
<td>150</td>
</tr>
<tr>
<td>7.2.4 Hearsay Under Federal Rules of Evidence 801 to 807</td>
<td>160</td>
</tr>
<tr>
<td>7.2.5 The Original Writing (Best Evidence) Rule (Federal Rules of Evidence 1001 to 1008)</td>
<td>166</td>
</tr>
<tr>
<td>7.2.6 Probative Value vs. Prejudice Under Federal Rule of Evidence 403</td>
<td>169</td>
</tr>
<tr>
<td>7.2.7 Judicial Notice Under Federal Rule of Evidence 201</td>
<td>170</td>
</tr>
<tr>
<td><strong>CHAPTER 8 Spoliation and Electronic Discovery Sanctions</strong></td>
<td>171</td>
</tr>
<tr>
<td>8.1 The Authority to Impose Sanctions</td>
<td>172</td>
</tr>
<tr>
<td>8.2 What Is Spoliation?</td>
<td>174</td>
</tr>
<tr>
<td>8.3 Conduct Giving Rise to Spoliation Sanctions Under Rule 37(e)</td>
<td>174</td>
</tr>
<tr>
<td>8.4 Examples of Spoliation Conduct for Which Sanctions Have Been Awarded</td>
<td>180</td>
</tr>
<tr>
<td>8.5 Examples of Other Electronic Discovery Misconduct Giving Rise to Sanctions</td>
<td>182</td>
</tr>
<tr>
<td>8.6 Types of Sanctions Available</td>
<td>182</td>
</tr>
<tr>
<td>8.7 Sanctions Imposed Against Outside Counsel</td>
<td>195</td>
</tr>
</tbody>
</table>
# TABLE OF CONTENTS (continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.8 The Independent Tort of Spoliation</td>
<td>200</td>
</tr>
<tr>
<td>8.9 Are Sanctions Inevitable?</td>
<td>203</td>
</tr>
<tr>
<td><strong>CHAPTER 9 Appendices</strong></td>
<td>205</td>
</tr>
<tr>
<td>9.1 Glossary of Common eDiscovery Terms</td>
<td>205</td>
</tr>
<tr>
<td>9.2 Petabyte, Terabyte, Gigabyte – What do these mean for eDiscovery?</td>
<td>226</td>
</tr>
<tr>
<td>9.3 eDiscovery Authorities</td>
<td>228</td>
</tr>
<tr>
<td>9.4 Overview of eDiscovery Statutes</td>
<td>274</td>
</tr>
<tr>
<td>9.5 Potential Sources of Information</td>
<td>299</td>
</tr>
<tr>
<td>9.6 Morgan Lewis eData Practice</td>
<td>301</td>
</tr>
</tbody>
</table>
CHAPTER 3
IDENTIFICATION AND PRESERVATION

As a general rule, a duty to preserve arises whenever there is a reasonable anticipation of litigation. In this
context, litigation includes not only traditional litigation but also proceedings before administrative
agencies or other regulatory bodies. Whenever such a duty arises, affirmative steps must be taken to
identify and preserve any unique, potentially relevant documents or electronically stored information (ESI)
in the party's possession, custody, or control. The volume and complexity of ESI implicated by this duty
have made compliance increasingly challenging, and sanctions for noncompliance have become
increasingly common.

3.1 When Does a Duty to Preserve Arise?

A duty to preserve arises whenever there is a reasonable anticipation of litigation.1 This is an objective
standard that asks whether a reasonable party faced with the same factual circumstances would have
reasonably anticipated litigation.2 Thus, "when a party 'has notice that the evidence is relevant to litigation
. . . or should have known that the evidence may be relevant to future litigation,"" the party has a duty to
preserve the evidence.3

Litigation need not be imminent or certain, nor must all contingencies to litigation have been resolved, for
litigation to be reasonably foreseeable.4 Indeed, "[i]t would be inequitable to allow a party to destroy

---

1. See Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC, 685 F. Supp. 2d 456, 466 (S.D.N.Y.
2010), abrogated in part on other grounds by Chin v. Port Auth. of N.Y. & N.J., 685 F.3d 135 (2d Cir. 2012); see also CAT3,
App. B-15 (Sept. 2014) (while rules do not create a duty to preserve, the rules take the duty as established by case law,
"which uniformly holds that a duty to preserve information arises when litigation is reasonably anticipated").
2. See Micron Tech., Inc. v. Rambus Inc., 645 F.3d 1311, 1320 (Fed. Cir. 2011).
F.3d 448, 459 (6th Cir. 2008)).
4. See Hynix Semiconductor Inc. v. Rambus, Inc., 645 F.3d 1336, 1346 (Fed. Cir. 2011); see also Micron, 645 F.3d at
1320 (reasonable foreseeability standard does not require that litigation be "imminent or probable without significant
contingencies").
documents it expects will be relevant in an expected future litigation, solely because contingencies exist, where the party destroying documents fully expects those contingencies to be resolved.\textsuperscript{5}

Nor must a party “understand[ ] the precise nature of the specific litigation at issue.”\textsuperscript{6} Instead, a party must simply have “notice that the documents might be relevant to a reasonably-defined future litigation.”\textsuperscript{7}

Because plaintiffs control the timing of a lawsuit, plaintiffs usually foresee litigation, and thus have a duty to preserve information before litigation commences.\textsuperscript{8} Conversely, an entity will not necessarily have anticipated litigation when there is a mere possibility, rumor, or indefinite threat of litigation.\textsuperscript{9}

There are many events from which a party may reasonably anticipate litigation such that a duty to preserve may be triggered. For example, some obvious triggers are the receipt of prelitigation preservation letters from counsel that specifically threaten litigation,\textsuperscript{10} service of a complaint\textsuperscript{11} or subpoena,\textsuperscript{12} or receipt of a notice of investigation from a federal agency or court.\textsuperscript{13} Triggers can also occur much earlier. For example, an employee’s filing of an Equal Employment Opportunity Commission (EEOC) charge may be a trigger.\textsuperscript{14} Other less obvious triggers may include the hiring of outside counsel;\textsuperscript{15} communications with outside counsel regarding initiation of litigation against others;\textsuperscript{16} an admission by an employee of a regulatory violation; the launch of an internal investigation;\textsuperscript{17} the suspension or termination of an

\begin{itemize}
  \item \textsuperscript{5} Hynix, 645 F.3d at 1346.
  \item \textsuperscript{7} See id. at *11.
  \item \textsuperscript{8} See Micron, 645 F.3d at 1321; Pension Comm., 685 F. Supp. 2d at 466; Crown Castle USA Inc. v. Fred A. Nudd Corp., 2010 WL 1286366, at *6, *10 (W.D.N.Y. Mar. 31, 2010); accord Hynix, 645 F.3d at 1346.
  \item \textsuperscript{13} See United States v. Quattrone, 441 F.3d 153, 162, 189-90 (2d Cir. 2006) (discussing duty to preserve when there were National Association of Securities Dealers and Securities and Exchange Commission investigations); In re Delta/AirTran Baggage Fee Antitrust Litig., 770 F. Supp. 2d 1299, 1308 (N.D. Ga. Fed. Feb. 22, 2011) (duty to retain documents because of Department of Justice (DOJ) investigation); Rimkus, 688 F. Supp. 2d at 612 (spoliation includes the destruction of evidence that may be relevant to a government investigation or audit); E*Trade Sec. LLC v. Deutsche Bank AG, 230 F.R.D. 582, 588 (D. Minn. 2005) (duty to preserve triggered when defendant received notice that bankruptcy court was investigating a fraudulent scheme).
  \item \textsuperscript{14} See Jones v. Breman High Sch. Dist. 228, 2010 WL 2106640, at *6 (N.D. Ill. May 25, 2010); Zubilule v. UBS Warburg LLC, 220 F.R.D. 212, 217 (S.D.N.Y. 2003) (Zubilule IV); see also Bynie v. Town of Cromwell, Bd. of Educ., 243 F.3d 93, 108 (2d Cir. 2001) (only logical to anticipate litigation when complaint was filed with Connecticut Commission of Human Rights and Opportunities).
  \item \textsuperscript{16} See Barsoum v. NYC Hous. Auth., 202 F.R.D. 396, 400 (S.D.N.Y. 2001).
  \item \textsuperscript{17} See Marceau v. Int’l Bhd. of Elec. Workers, 618 F. Supp. 2d 1127, 1174-77 (D. Ariz. 2009) (leaving for trial the
employee for cause;\textsuperscript{18} the receipt of multiple objections or complaints;\textsuperscript{19} the filing of other lawsuits with the same or similar facts;\textsuperscript{20} the receipt of a complaint regarding the unauthorized use of a product;\textsuperscript{21} an employee’s complaining of discrimination, harassment, or sexual assault;\textsuperscript{22} the termination of a contract after a dispute arises between the parties to the contract;\textsuperscript{23} the failure of attempts to resolve a matter through negotiations or mediation;\textsuperscript{24} the occurrence of an accident causing serious injury or death;\textsuperscript{25} knowledge in the industry of likely claims or receipt of media attention;\textsuperscript{26} or a tender of notice to an insurance carrier.

**Practice Pointer: The Shifting Duty of Preservation**

- Parties subject to frequent, repeat litigation may become concerned about whether the duty to preserve documents in one investigation or litigation can be extended to another litigation. While courts may sometimes consider whether there was an independent duty to preserve information, this duty “does not necessarily mean that it had such a duty with respect to the litigation, and the fact that the party failed to observe some other obligation does not itself prove that its efforts to preserve were not reasonable with respect to a particular case.”\textsuperscript{27} Whether the duty can be shifted will often depend upon whether a previous litigation hold was issued for the benefit of the new litigant.

- In *In re Actos*,\textsuperscript{28} the defendant argued that there should be no shifting duty of preservation from a hold issued in 2002 because the defendant did not reasonably anticipate new litigation with the 2010 multidistrict litigation (MDL) plaintiffs. The court disagreed, finding that the defendant had issued and refreshed a general products liability litigation hold instructing employees to preserve any documents related to the specific drug at issue in the MDL. Thus, the duty to preserve documents as to the claims of the MDL plaintiffs arose back when prior holds were issued.

\begin{itemize}
\item 18. See Zbylski, 154 F. Supp. 3d 1146, 1164 (duty to preserve triggered no later than date teacher was put on administrative leave).
\item 20. See *In re Ethicon, Inc. Pelvic Repair Sys. Prod. Liab. Litig.* 299 F.R.D. 502, 516-18 (S.D. W. Va. 2014) (when notice for new litigation referenced ongoing duty from prior litigations, duty to preserve had already arisen before new litigation); see also Rimkus, 688 F. Supp. 2d at 607; Stevenson v. Union Pac. R.R. Co., 354 F.3d 739, 748 (8th Cir. 2004); Lewy, 836 F.2d at 1112. But see *Point Blank Sols.*, Inc. v. Toyobo Am., Inc., 2011 WL 1456029, at *22-24 (S.D. Fla. Apr. 5, 2011) (finding there is no shifting duty from one claim to another where different individuals are owed the duty of preservation).
\item 25. See Stevenson, 354 F.3d at 748; see also *Blinzler v. Marriott Int’l, Inc.*, 81 F.3d 1148, 1159 (1st Cir. 1996).
\item 26. See *Phillip M. Adams & Assoc., L.L.C. v. Dell, Inc.*, 621 F. Supp. 2d 1173, 1191 (D. Utah 2009). But see *Point Blank*, 2011 WL 1456029, at *22-24 (leaving for another day whether there is a duty to preserve if a party is on notice of industrywide litigation).
\end{itemize}
Conversely, in *Point Blank*, the court rejected a shifting duty argument, noting that a preservation duty is owed to a specific party. The obligations to preserve documents in another litigation and in response to a subpoena issued by the government did not mean that the defendant anticipated the new litigation with the plaintiff. Thus, there could be no “shifting duty” to preserve documents.

Adopting a Process for Evaluating Whether Litigation Is Reasonably Anticipated

Organizations should consider adopting a process for evaluating whether litigation is reasonably anticipated such that a duty to preserve has arisen. Such an evaluation process can help demonstrate that the client made a defensible decision. As Shira A. Scheindlin, former District Judge for the Southern District of New York, noted, one of the questions a court may ask when deciding whether litigation was reasonably anticipated is “Did an organization create a process for evaluating the threat of litigation?” As part of the evaluation process, an ultimate decisionmaker must decide, in light of the facts and circumstances, whether litigation is anticipated. While such a decision “is fact-intensive and is not amenable to a one-size-fits-all or a checklist approach,” an organization should develop trigger guidelines to assist the ultimate decisionmaker in evaluating whether litigation is reasonably anticipated.

Practice Pointer: Evaluating Policies and Processes

- Companies should consider developing “trigger guidelines” that provide management with guidance and examples of situations that may trigger a duty to preserve. These guidelines can be included in an Information Governance Program or a Discovery Manual and Playbook, which were discussed in detail in Chapter 2, Information Governance.
- Among other things, companies should examine the organization’s litigation history, HR and ethics policies, and reporting obligations to identify those policies and procedures that could dovetail with “reasonable anticipation” of litigation. One example is the work-product doctrine.

Consistency Between the Preservation Duty and Work Product

As a practical matter, a party should beware of falling into the trap of claiming one date for preservation and another date for when work product was created for the case. Because both the duty to preserve and the work-product immunity arise when litigation is reasonably anticipated, a party must ensure consistency between the dates claimed for the duty of preservation and the work-product immunity. As

---

30. Other cases following the *Point Blank* rationale include *In re Delta/AirTran Baggage Fee Antitrust Litigation*, 770 F. Supp. 2d 1299 (duty to preserve documents as a result of a DOJ demand did not mean the defendant owed the same duty to the plaintiffs), and *Stanfill v. Talton*, 851 F. Supp. 2d 1346 (M.D. Ga. 2012) (finding that even if defendant owed a duty of preservation to the government as a result of an investigation, it did not owe that duty to the plaintiff).
one judge in the Eastern District of New York found, if litigation is reasonably foreseeable for work-product purposes, it is reasonably foreseeable for preservation purposes. However, if a party is confronted with a situation where work product is claimed before the issuance of a litigation hold, the party should consider whether it can argue that the work product was generated in preparing for another lawsuit.

**Court-Ordered Preservation**

Once litigation has commenced, a judge may issue an order setting forth specific preservation requirements for that case. Such instructions may be issued in a standing order or prior to any initial status conference. Early meet-and-confer efforts, however (for example, prior to the Federal Rule of Civil Procedure (Federal Rule) 26 conference), may serve to limit such instructions if issued after the parties have appeared.

**Preservation Demand Letters**

Parties also may issue letters to other litigants or third parties informing them of their preservation obligations and specifying that data or systems that are likely to contain information relevant to the matter at hand must be preserved. Government agencies also may include such information in subpoenas or other requests for information. It is a best practice to immediately review such requests or instructions and determine if it is possible and/or necessary to comply in light of the issues in the matter and current law governing electronic discovery. A meet and confer should follow.

### 3.2 What Must Be Preserved?

As a general rule, parties are required to preserve documents or ESI in their possession, custody, or control that are potentially relevant and unique. This is an ongoing duty that supersedes usual records management policies.

#### 3.2.1 Guidance from the Federal Rules

Although the Federal Rules do not create the preservation obligation, which is a matter of common law (or in some areas imposed by statute or regulation), they guide the scope of preservation by establishing the scope of potential discovery.

---

37. See Point Blank, 2011 WL 1456029, at *24 (mere fact that documents created in 2003 were placed on privilege log did not warrant finding that party had a duty to preserve documents as of that point in time because defendants created documents as a result of another lawsuit and government investigation).
41. See Cache, 244 F.R.D. at 629; Zubulake IV, 220 F.R.D. at 218.
43. Various federal regulations include a duty to preserve records. See, e.g., Byrnie, 243 F.3d at 108-09 (party had duty to preserve documents under EEOC records-retention regulation); Dupee v. Klaff’s, Inc., 462 F. Supp. 2d 244, 249 (D. Conn. 2006) (employer had duty to preserve documents under Family and Medical Leave Act); 29 U.S.C. § 657(c)(1) (requiring...
First, Rule 26(b)(1) establishes the general scope of discovery:

Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party’s claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties’ relative access to relevant information, the parties’ resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit. Information within this scope of discovery need not be admissible in evidence to be discoverable.

Since the potential scope of discovery is broad—encompassing anything relevant and proportional to the needs of the case—the scope of preservation must be similarly broad.

Second, Rule 34(a) specifies that a party can propound a discovery request, within the limits of Rule 26, requesting “any designated documents or electronically stored information” that is “in the responding party’s possession, custody, or control.” This parameter also broadens the preservation obligation into one that extends beyond the information within a party’s physical possession into that which is in its custody or control. 44 This requirement is examined in further detail in Section 3.2.3, Possession, Custody, or Control.

Finally, Rule 26(b)(2)(C) states that “the court must” limit the scope of discovery if “discovery sought is unreasonably cumulative or duplicative.” From this, the courts have inferred the limitation to preserve only those documents that are unique. 45

3.2.2 “Electronically Stored Information” and Its Potential Sources

As noted above, discovery and preservation extend to documents or ESI. The Federal Rules intentionally avoid defining the term “electronically stored information” with precision in order to accommodate “[t]he wide variety of computer systems currently in use, and the rapidity of technological change.” 46 In other words, the amended Federal Rules envision the discovery of “any type of information that is stored electronically,” 47 including forms of ESI not yet invented.

Given the breadth of discovery and the wide-ranging use of technology in business today, litigants may need to look in a long list of places for potentially relevant data. Each case is likely to implicate a different subset of sources depending on its subject matter (e.g., an employment discrimination matter might
implicate HR data and email but have nothing to do with marketing or operations data). Thus, a company should consider the sources of information that are likely to be relevant to the case and focus its efforts on those sources of ESI. To assist the company in its assessment, it is advantageous to maintain a master list of all potential data sources within the company.

The following is an example of a list of potential sources to be considered, including brief descriptions of each source:

**Email**

**Microsoft Outlook - .pst**
- Runs on Exchange servers
- Local .pst files

**Lotus Notes - .nsf**
- Runs on Domino servers
- Mostly resides on servers
- Can be locally replicated

**Webmail**
- Gmail, Yahoo! Mail, AOL, etc.
- Lives on hosted servers – ISP
- Office 365
- Cloud-based email and productivity suite hosted by Microsoft

**Servers**
- Stored on network devices, such as file servers
- Usually the same kind of data files as found on a PC: unstructured data, such as Microsoft Word documents, Excel spreadsheets, and PowerPoint presentations
- Either shared or personal
- Some organizations have document-management systems

**Hard drives**

**Personal computer hard drive—typically contains:**
- Data files – Microsoft Office (Word, Excel, PowerPoint)
- Locally stored email in .pst or .nsf files
- System files – make the computer run and are generally not relevant in discovery
- Internet cache files – auto downloads that help you surf the Web and house Web history, cookies, and temporary Internet files
- Deleted files – many “deleted” files can still be retrieved from computer hard drives using forensic tools. While a user may think that a deleted file is gone, the computer simply marks the space occupied by the file as available. It does not delete the file; therefore, the file can be resorted fairly easily. The space where deleted files can be found is often referred to as “slack” or “unallocated” space.
Other communication tools

- Instant messaging – transcripts may be stored on individual users’ machines or company servers depending on which tool is in use and how it is configured
- Blogs – online diaries
- Chat rooms – bulletin boards and online locations for users of common interest to communicate online
- Text messaging – typed messages sent via cell phone or PDA; not stored by service provider and typically limited storage on device
- Digital phone (VoIP) and voicemail – digital voicemail is ESI

Social media

- Facebook
- Twitter
- LinkedIn
- Instagram
- Snapchat
- Countless other user-controlled websites and apps for communicating, journaling, and otherwise sharing personal information

Databases

- Also known as structured data
- Document storage and information archiving and manipulation
- Typically accessed by many users
- Information updated regularly
- Usually have reporting capability

Mobile devices

- Smartphones
- BlackBerrys
- iPods, MP3 players
- Portable storage devices and media – CDs, thumb drives, portable hard drives

Cloud

- Amazon Web Services, Microsoft Azure
- Salesforce
- Dropbox, Syncplicity, Google Drive, iCloud
Other

- Backups
- Keycard access logs
- Security camera footage
- Photocopier hard drives
- Voice recordings from recorded phone lines
- Always ask the question, “Are there other sources we haven’t considered?”

**Practice Pointer: Backups**

Backups (whether on tape, on media, or in virtual environments) are a storage format commonly used to back up servers and other data sources for archival storage or disaster recovery. Backups can often hold hundreds of gigabytes—if not terabytes—of data. Large organizations may require multiple media to complete each backup, and it often can be costly and time-consuming to restore, index, and search for relevant material. Additionally, it is common for companies to recycle backups on a regular schedule (e.g., reusing the same single set at the end of each week or having four sets in rotation so that each backup is available for a month before being overwritten).

In order to determine whether backups should be preserved, a party must first consider whether the backups are accessible, i.e., actively used for information retrieval, or inaccessible, i.e., typically maintained solely for the purpose of disaster recovery. As a general rule, a party should preserve accessible backups, but it need not preserve inaccessible backups even when it reasonably anticipates litigation. This general rule that inaccessible backups need not be preserved flows from the concept that a party need not preserve every identical copy of information. Because backups typically maintain data that is wholly duplicative of data found in more readily accessible sources to be preserved, backups can generally be excluded from preservation when a legal hold is timely implemented and sufficient to preserve potentially relevant data in active information systems.

---

48. See *Zubulake IV*, 220 F.R.D. at 218.

49. See id.; see also *Starbucks Corp. v. ADT Sec. Servs., Inc.*, 2009 WL 4730798, at *6 (W.D. Wash. Apr. 30, 2009) (when ADT argued that its archival “Plasmon” system was inaccessible and costly to restore, the court found it accessible because personnel continued to use the system).

50. See *Zubulake IV*, 220 F.R.D. at 218 ("As a general rule, that litigation hold does not apply to inaccessible backup tapes (e.g., those typically maintained for the purpose of disaster recovery), which may continue to be recycled on the schedule set forth in the company's policy. On the other hand, if the backup tapes are accessible (i.e., actively used for information retrieval), then such tapes would likely be subject to the litigation hold . . . ."); see also *Automated Sols. Corp. v. Paragon Data Sys., Inc.*, 756 F.3d 504, 514-15 (6th Cir. 2014) (discussing *Zubulake IV* in upholding finding that inaccessible backups were not subject to the duty to preserve); The Sedona Conference®, Sedona Principles Addressing Electronic Document Production (2d ed.), Principle 5, cmt. 5h ("absent specific circumstances, preservation obligations should not extend to disaster recovery tapes created in the ordinary course of business").

51. See *Zubulake IV*, 220 F.R.D. at 218.

52. See *Gaalla v. Citizens Med. Ctr.*, 2011 WL 2115670, at *1-2 (S.D. Tex. May 27, 2011) (party did not violate its preservation duty when it continued to recycle backup tapes because it had issued a litigation hold to employees after the filing of lawsuit and had taken snapshots of relevant email accounts); see also *MRT, Inc. v. Vounckx*, 299 S.W.3d 500, 510-11 (Tex. Ct. App. – Dallas 2009) (refusing to find that a party had a duty to preserve backup tapes maintained for disaster recovery purposes when there was nothing to indicate that the tapes contained relevant information deleted from active data.
However, if a party can identify the backups that are storing the key players’ documents and that information is not otherwise available, the backups should be preserved.\(^{53}\)

Additionally, the Zubulake V court specifically provided that any backups required to be preserved should be segregated from others to avoid their inadvertent destruction.\(^{54}\) In addition, a party should suspend the routine overwriting of such backups.\(^{55}\)

### 3.2.3 Possession, Custody, or Control

Federal Rule of Civil Procedure 34(a)(1) specifies that parties may only request the production of documents or ESI “in the responding party’s possession, custody, or control.” This is just as true in the context of ESI as it is for physical records.

ESI is within a party’s possession, custody, or control not only when the party has actual possession or ownership of the information, but also when the party has “the legal right to obtain the documents on demand.”\(^{56}\) Such a legal right will be found where there are contractual provisions granting a right of access to documents.\(^{57}\) A legal right to obtain information upon demand can also be established through the existence of a principal-agent relationship, such as a relationship between an employer and employee, a client and an attorney, or a corporation and an officer or director.\(^{58}\)

In addition, some jurisdictions have found that documents are under a party’s control when the party has the “practical ability to obtain the documents from a non-party to the action.”\(^{59}\) For example, when a third


\(^{56}\) See Flagg v. City of Detroit, 252 F.R.D. 346, 353 (E.D. Mich. 2008); see also S.E.C. v. Strauss, 2009 WL 3459204, at *8 (S.D.N.Y. Oct. 28, 2009) (control will exist when party has the right to access documents pursuant to a contract).


\(^{58}\) Bank of N.Y. v. Meridien BIAO Bank Tanzania Ltd., 171 F.R.D. 135, 146 (S.D.N.Y. 1997); see also Strauss, 2009 WL 3459204, at *7 (party has control over material that it has the practical ability to obtain and over material that it has the legal right to obtain); Tomlinson v. El Paso Corp., 245 F.R.D. 474, 477 (D. Colo. 2007) (documents are within a party’s control “if such party has retained any right or ability to influence the person in whose possession the documents lie”). But see Phillip M. Adams & Assoc., L.L.C. v. Dell, Inc., 2007 WL 626355, at *3 (D. Utah Feb. 22, 2007) (noting how district courts have rejected the “practical ability” test); The Sedona Conference®, The Sedona Conference Commentary on Rule 34 and Rule 35 “Possession, Custody, or Control,” at 1 (Apr. 2015) (“This Commentary is to advocate abolishing use of the common-law ‘practical ability test’ for purposes of determining Rule 34 and Rule 45 ‘control’ of Documents and ESI.”).
party received a majority of its revenues from an organization, the court found that the organization likely had the ability to influence the third party into producing documents.60

Because the duty of preservation extends to any information within the party’s possession, custody, or control,61 counsel may need to look beyond the client to third parties for potential document preservation, including third-party administrators of computer systems,62 third-party phone and text service providers,63 third-party payroll vendors,64 third-party administrators of retirement plans,65 third-party administrators of repair plans,66 former employees,67 current or former outside counsel,68 accountants,69 independent officers or directors,70 related entities,71 a joint venture or partnership to which the client belongs,72

60. See Jacoby v. Hartford Life & Accident Ins. Co., 254 F.R.D. 477, 479 (S.D.N.Y. 2009) (when third party received 75% of its revenues from defendant, defendant likely had control because of its ability to use its influence to obtain documents).
61. See In re NTL, 244 F.R.D. at 195-97 (defendant had a duty to preserve documents held by a spin-off corporation, as documents were within its control); Arteria Prop., 2008 WL 4513696, at *5 (duty to preserve content posted on website hosted by a third-party web design company because content on website was under defendant’s control). But see Phillips v. Netblue, Inc., 2007 WL 174459, at *1-3 (N.D. Cal. Jan. 22, 2007) (hyperlinks to third-party websites not in possession, custody, or control of party).
62. See In re NTL, 244 F.R.D. at 198 (noting failure of party to inform outsourcing vendor of litigation hold); Arteria Prop., 2008 WL 4513696, at *5 (finding an adverse inference was warranted when website was destroyed after litigation commenced because defendant had control over website). Columbia Pictures, Inc. v. Bunnell, 245 F.R.D. 443, 453 (C.D. Cal. 2007) (information routed through third-party server when individual accessed defendant’s website was within defendant’s possession, custody, or control).
63. See Flagg, 252 F.R.D. at 352.
67. See Pension Comm., 685 F. Supp. 2d at 465, 482 n.125 (party may have had duty to collect information from former employee “assuming it had the ‘practical ability to do so’”); Cache, 244 F.R.D. at 625 (discussing failure to contact former employees to identify and collect responsive materials); accord In re Folding Carton Antitrust Litig., 76 F.R.D. 420, 423 (N.D. Ill. 1977) (defendants who continued to pay former employee in cash or in kind had control because “[w]hile the right to withhold payment does not ipso facto mean that defendants will be able to procure the documents, it is clearly an indicia of control”). In re Auction Houses Antitrust Litig., 196 F.R.D. 444, 445-46 (S.D.N.Y. 2000) (information within former CEO’s possession was within company’s control because termination agreement provided for compliance with request made to CEO concerning civil litigation). But see Kickapoo Tribe of the Indians of the Kickapoo Reservation in Kan. v. Nemaha Brown Watershed Jt. Dist. No. 7, 294 F.R.D. 610, 613-14 (D. Kan. 2013) (documents in possession of former employees, staff, and board members were not in possession, custody, or control of defendant).
72. See Kannatan v. BenQ Corp., 2005 WL 2455825, at ¶5-6 (E.D. Tex. Oct. 4, 2005) (party that held 49% of joint venture had control over joint venture’s documents); In re Subpoena Duxes Tecum Served on Duke Energy Corp., 2005 WL 2674938, at ¶4-5 (W.D.N.C. Oct. 18, 2005) (Duke Energy had “control” over documents held by its subsidiary’s joint venture when the subsidiary owned 60% of the joint venture); In re Hallmark Capital Corp., 534 F. Supp. 2d 981, 983 (D. Minn. 2008) (partner in partnership required to produce partnership documents within partner’s control).
members of a limited liability company or joint venture or partnership,73 trustees,74 and vendors or contractors.75

Social media can also create unique possession, custody, or control issues. For example, when a party is tagged in photos posted by another, the party may be deemed to be in possession, custody, or control of that information.76

Implementation of Bring Your Own Device (BYOD) policies and use of personal devices can further complicate a party’s preservation obligations. Whether the entity issues the devices or employees are allowed to use their own devices for work-related purposes, the employer will likely have a duty to preserve work-related information on the devices as being under the employer’s control.77

New technology has raised additional questions about the application of this principle in the context of ESI, as many third-party technology service providers or cloud computing services possess an enterprise’s data.78 So far, the case law indicates that data a company can obtain on demand from a third party is within the company’s “control.”

For example, in Arteria Property PTY Ltd. v. Universal Funding V.T.O., Inc., the court found that the defendant had a duty to preserve content on a website maintained by a third party web design company because the defendant “had the ultimate authority, and thus control, to add, delete, or modify the website’s content.”79 Similarly, in Flagg v. City of Detroit, the court held that a defendant was obligated to

73. See City of Seattle, 2008 WL 539809, at *2 (finding LLC had a right to obtain documents upon demand from its members because members were managers and thus agents under Oklahoma law); Starlight Int’l Inc. v. Herlihy, 186 F.R.D. 626, 635 (D. Kan. 1999) (joint venture had legal right to obtain documents from members); Nat’l Council on Compensation Ins., Inc. v. Am. Int’l Grp., Inc., 2007 WL 4365371, at *3 (N.D. Ill. Dec. 11, 2007) (association required to produce documents within possession of its members). But see In re NCAA Student-Athlete Name & Likeness Litig., 2012 WL 161240, at *1-5 (N.D. Cal. Jan. 17, 2012) (organization did not have control over member institution documents).

74. See Hamstein Cumberland Music Grp. v. Estate of Williams, 2008 WL 2682697, at *3 (N.D. Okla. June 30, 2008) (documents in trustee’s possession were within trust grantor’s control when grantor established a revocable trust).

75. See Sedona Corp. v. Open Sols., Inc., 249 F.R.D. 19, 22 (D. Conn. 2008) (defendant controlled documents held by third-party contractor because agreement gave the defendant the right to obtain materials upon request); Ice Corp. v. Hamilton Sundstrand Corp., 245 F.R.D. 513, 518-19 (D. Kan. 2007) (finding third-party product design information within custody or control of litigant, as agreement noted that designs “shall at all times remain vested” in litigant); Mercy Catholic Med. Ctr. v. Thompson, 380 F.3d 142, 160 (3d Cir. 2004) (subcontractor audit documents within possession, custody, or control when Medicare manuals required that records be made available to contractor); Mercy Catholic Med. Ctr. v. Thompson, 380 F.3d 142, 160 (3d Cir. 2004) (subcontractor audit documents within possession, custody, or control when Medicare manuals required that records be made available to contractor); Nw. Pipeline Corp. v. Ross, 2008 WL 1744617, at *4-5 (W.D. Wash. Apr. 11, 2008) (party had to produce bore log in possession of third-party contractor when contractor created bore log at request of party).

76. See Higgins v. Koch Dev., 2013 WL 3366278, at *3 (S.D. Ind. July 5, 2013) (when the plaintiff was tagged in photos posted by others, the photos became part of the plaintiff’s Facebook timeline, and, therefore, were within the plaintiff’s possession, custody, or control).

77. See Cotton v. Costco Wholesale Corp., 2013 WL 3819974, at *6 (D. Kan. July 24, 2013) (finding defendant did not have within its possession, custody, or control text messages sent or received by individuals on their personal cell phones because defendant did not issue cell phones and nothing evidenced that employees used cell phones for work-related purposes); see also In re Pradaxa (Dabigatran Etxelate) Prods. Liab. Litig., 2013 WL 6486921, at *16-18 (S.D. Ill. Dec. 9, 2013), rescinded on other grounds, In re Petition of Bouringer Ingelheim Pharm., Inc., 745 F.3d 216 (7th Cir. Jan. 24, 2014) (when party directed sales force to communicate with supervisors and managers via cell phones and texts, party had duty to preserve text messages not only on those phones issued by the company but also on personal cell phones); Small v. Univ. Med. Ctr. of S. Nev., 2014 WL 4079507, at *10-11, *28 (D. Nev. Aug. 18, 2014) (Special Master finding that party failed to preserve personal mobile devices that employees used for work even though custodians initially responded that they did not use personal devices for work as analysis of signature lines in relevant data showed they did).


produce text messages stored with its third-party service provider because they were within the defendant’s control. Another example can be found in Tomlinson v. El Paso Corp., where the court held that a company had control of certain electronic ERISA records maintained for the company by a third-party service provider and, therefore, had to produce them.

On the flip side, third-party service providers may also be forced to produce the documents of their customers because such information is within the service providers’ control.

Even if materials in the hands of third parties are not within a party’s possession, custody, or control, the party may still have a duty to notify the opposing side of evidence located in the hands of third parties.

**Practice Pointer: Protecting Data Assets During Mergers, Acquisitions, and Reorganizations**

The duty to preserve documents does not disappear when there is a subsequent reorganization, sale of a company, or sale of relevant assets. In Pegasus Aviation I, Inc. v. Varig Logistica S.A., one group of defendants had purchased another defendant out of Brazilian bankruptcy, and in so doing, was ordered to “manage and administer” the bankrupt defendant. The court found that the purchasing defendants had sufficient control over the bankrupt defendant to trigger a duty on the purchasing defendants’ part to preserve the bankrupt entity’s ESI. Similarly, in In re NTL, Inc. Securities Litigation, the defendant filed for bankruptcy and emerged from the bankruptcy plan as two different companies: one company was the successor-in-interest for the purposes of the lawsuit while the other company obtained the relevant documents and assets of the original debtor. The company obtaining the relevant documents destroyed them, and the court sanctioned the defendant for spoliation of documents within its control. In Centimark Corp. v. Pegnato & Pegnato Roof Management, Inc., the defendant sold assets after litigation commenced. As part of the sale, the defendant turned over relevant documents to the third-party purchaser, which, in turn, lost or destroyed the documents. The defendant was held responsible for spoliation as a result of the purchaser’s conduct.

To avoid the sanctions faced by the defendants in Pegasus, Centimark and In re NTL, a party selling assets should do the following:

1. Retain a copy of any data relevant to an ongoing or reasonably anticipated litigation.
2. Give the opponent access to the documents before the sale or reorganization.

3. Contractually ensure that the purchaser will retain the data for as long as needed for the litigation, that the company will have access to the data after the completion of the sale or reorganization, and that such access will allow for the production of data to the opposing side in ongoing or reasonably foreseeable litigation.

In the same way, if an organization acquires a business or assets, courts will likely presume that the organization had possession, custody, or control of documents possessed by its predecessor. For this reason, an organization acquiring a business or its assets should conduct due diligence on the target’s preservation and disposition practices.

### 3.2.4 Limitations on What Must Be Preserved

The preservation obligation is very broad, though not limitless. The courts have recognized that preserving every copy of every paper or every piece of electronic data would impose an undue burden on an enterprise. A party that anticipates litigation must retain unique, relevant information: “[a] party or anticipated party must retain all relevant documents (but not multiple identical copies) in existence at the time the duty to preserve attaches, and any relevant documents created thereafter.”

Currently, a party faced with a burdensome and costly preservation obligation does not have any automatic relief available to it. Instead, the party must seek relief from such obligation through negotiating with the opposing party and/or securing an order from the court.

**Relevant Inaccessible Data Should Be Retained**

While the Federal Rules provide for limitations on production of inaccessible data to avoid undue burden, those limitations do not apply to preservation, though one might be able to obtain relief under the proportionality standard discussed below. Both accessible and inaccessible data must be preserved absent an agreement or court order relieving the party of such obligation:

> A party’s identification of sources of electronically stored information as not reasonably accessible [on account of undue burden or expense] does not relieve the party of its common-law or statutory duties to preserve evidence. Whether a responding party is required to preserve unsearched sources of potentially responsive information that it believes are not reasonably accessible [because of

---


88. See *Zubulake IV*, 220 F.R.D. at 217.

89. *Id.* at 218.

90. See *In re Seroquel Prods. Liab. Litig.*, 244 F.R.D. 650, 656 (M.D. Fla. 2007).
undue burden or expense] depends on the circumstances of each case. It is often useful for the parties to discuss this issue early in discovery.\textsuperscript{91}

Moreover, the Federal Rules make clear in Rule 26(b)(2)(B) that even burdensome production can be ordered for good cause, which presupposes that the burdensome records are being preserved in case production is later ordered. Thus, the fact that the relevant data is located in a source that may make it difficult or expensive to preserve does not diminish a litigant’s preservation obligations.\textsuperscript{92}

**Proportionality Limiting the Scope of Preservation**

The Federal Rules may provide for one other potential source of relief in Rule 26, which limits discovery to relevant information that is “proportional to the needs of the case.” Rule 26 supplies a balancing standard, “considering the importance of the issues at stake in the action, the amount in controversy, the parties’ relative access to relevant information, the parties’ resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit.” Moreover, Rule 37(e) requires a party take “reasonable steps” to preserve ESI, which may be assessed by evaluating proportionality.\textsuperscript{93}

Courts are discussing the principle of proportionality in the context of preservation. As Judge Lee Rosenthal of the United States District Court for the Southern District of Texas has stated,

> Whether preservation or discovery conduct is acceptable in a case depends on what is reasonable, and that in turn depends on whether what was done—or not done—was proportional to that case and consistent with clearly established applicable standards.\textsuperscript{94}

Thus, the reasonableness of preservation efforts should be proportional to the amount in controversy and the costs and burdens of preservation.\textsuperscript{95}

Still, proportionality can be an amorphous standard that is difficult to apply.\textsuperscript{96} While parties may try to agree on the scope of reasonable and proportional preservation, absent such an agreement, a party may

\textsuperscript{91} Fed. R. Civ. P. 26 advisory committee’s note (2006).

\textsuperscript{92} See, e.g., In re Brand Name Prescription Drugs Antitrust Litig., 1995 WL 360526, at *2 (N.D. Ill. June 15, 1995) (holding that defendant must bear the burden and expense of preserving and ultimately producing relevant information to plaintiffs even though those efforts would be costly, given that “the necessity for a retrieval program or method is an ordinary and foreseeable risk” associated with keeping information in the form chosen by defendant); Toledo Fair Hous. Ctr. v. Nationwide Mut. Ins. Co., 703 N.E.2d 340, 354 (Ohio C.P. 1996) (a “party cannot avoid discovery when its own recordkeeping system makes discovery burdensome”); see also The Sedona Conference®, The Sedona Principles: Best Practices Recommendations and Principles for Addressing Electronic Document Production, cmt. 5.b (Annotated 2004) (“Organizations Must Prepare for Electronic Discovery to Reduce Cost and Risk.”).

\textsuperscript{93} See Fed. R. Civ. P. 37 advisory committee’s note (2015) (“Another factor in evaluating the reasonableness of preservation efforts is proportionality.”).

\textsuperscript{94} Rinkus, 688 F. Supp. 2d at 613.

\textsuperscript{95} See Victor Stanley, 269 F.R.D. at 522; see also Rinkus, 688 F. Supp. 2d at 613 n.8 (preservation should be proportional to the amount in controversy and the nature of the case).

\textsuperscript{96} Orbit One Commc’ns, Inc. v. Numerex Corp., 271 F.R.D. 429, 436 (S.D.N.Y. 2010) (citing Zubulake IV, 220 F.R.D. at 218) (noting that proportionality is an amorphous concept and advising litigants to retain all relevant documents because it “seems unlikely, for example, that a court would excuse the destruction of evidence merely because the monetary value of anticipated litigation was low”).

Chapter 3  **Identification and Preservation**  43
seek court intervention with respect to the scope of preservation. Ultimately, if a party chooses not to preserve information because of proportionality concerns, the party must be prepared to demonstrate that it acted in good faith by explaining the specific burden and cost associated with preserving the material along with an explanation of why the information is of little benefit.

3.3 How Should ESI Be Preserved?

Once a duty to preserve has been identified, and the scope of what must be preserved has been considered, clear instructions to preserve information must be provided to those individuals who are likely to have relevant information. The duty to preserve documents “runs first to counsel,” thus, counsel has an affirmative duty to effectively communicate discovery obligations to a client, including the duty to identify, retain, and produce documents. As part of this effort, counsel and the client must immediately distribute a legal hold.

FAQs

What is a legal hold?

A legal hold is the affirmative obligation to preserve records that might be relevant to actual or potential litigation, investigations, or other legal proceedings.

What triggers a legal hold?

A legal hold is triggered when it is known or reasonably should be known that certain records may constitute relevant evidence in actual or potential litigation, investigations, or other legal proceedings.

97. See Fed. R. Civ. P. 37 advisory committee’s note (2015) (“Once litigation has commenced, if the parties cannot reach agreement about preservation issues, promptly seeking judicial guidance about the extent of reasonable preservation may be important.”).

98. See id. (2015) (“A party urging that preservation requests are disproportionate may need to provide specifics about these matters in order to enable meaningful discussion of the appropriate preservation regime”); see also Pippins v. KPMG LLP, 279 F.R.D. 245, 255 (S.D.N.Y. 2012) (while proportionality is a factor in determining preservation obligations, when defendant only provided information regarding the alleged burden but failed to provide any information regarding the benefit of information, the defendant had a duty to preserve the information); Digital Vending Servs. Int’l, Inc. v. Univ. of Phoenix, Inc., 2013 WL 5533233, at *5 (E.D. Va. Oct. 3, 2013) (duty to preserve flash drive was proportional because “the scope of this litigation is such that the duty to preserve is proportionally very high”); Victor Stanley, 269 F.R.D. at 528 (noting that proportionality and reasonableness were not at issue because party never alleged that it would have been an undue burden to preserve information); accord PTSI, Inc. v. Haley, 2013 WL 2285109, at *11-13 (Pa. Super. Ct. May 24, 2013) (applying state proportionality standard when evidence was lost to determine that party was not entitled to discovery sanction); cf. Boeynams v. LA Fitness Int’l LLC, 2012 WL 3536306 (E.D. Pa. Aug. 16, 2012) (when party provided specific information about the costs of discovery as well as sampling some documents to show relative lack of relevance, court shifted cost of discovery); Seger v. Ernest-Spencer Metals, Inc., 2010 WL 378113, at *2 (D. Neb. Jan. 26, 2010) (when claiming undue burden, there is an obligation to provide detail about the nature of the burden in terms of time, money, and procedure).


103. See Zubulake IV, 220 F.R.D. at 218.

104. See, e.g., id. at 216; see also Fujitsu Ltd. v. Fed. Express Corp., 247 F.3d 423, 436 (2d Cir. 2001) (citing Kronisch v. United States, 150 F.3d 112, 126 (2d Cir. 1998)).
When does an organization “reasonably anticipate” litigation?

Reasonable anticipation of litigation has been described as the moment when:

- It is more likely than not that litigation will ensue
- A credible threat of litigation exists

A party should examine the facts and circumstances, as well as its experience, in making this determination.

3.3.1 Obligation to Issue a Written Legal Hold Notice

The first and most important step in fulfilling a duty to preserve is the issuance of a written legal hold notice. The importance of issuing a written legal hold notice has been discussed in prominent cases, and failure to do so is often one factor courts consider in determining whether sanctions should issue.

3.3.2 Elements of a Legal Hold Notice

To be effective, a legal hold notice needs to do several things with specificity. General admonitions to hold documents that do not provide sufficiently specific instruction to custodians have been found to be inadequate. A legal hold notice should include the following elements:

- **Clearly instruct individuals not to destroy records.** The hold should include language such as “immediately suspend the destruction of any responsive paper or electronic documents or data.”

- **Describe the substantive scope of what must be preserved.** This is the most important element; custodians must be affirmatively told to preserve and what to preserve. Without a clear description of the matter and the subjects it implicates, custodians cannot be certain what should and what should not be preserved.

---

105. See Pension Comm., 685 F. Supp. 2d at 465; see also Passlogix, 708 F. Supp. 2d at 410 (counsel must put in place a litigation hold and communicate that to employees); Zubulake V, 229 F.R.D. at 439 (“counsel must put in place a litigation hold and make that known to all relevant employees by communicating with them directly”); Keithley v. Homestore.com, Inc., 2008 WL 3833384, at *6 (N.D. Cal. Aug. 12, 2008) (lack of written legal hold exemplified defendant’s “lackadaisical attitude” with respect to preservation); In re Old Banc One Sh’holders Sec. Litig., 2005 WL 3372783, at *3 (N.D. Ill. Dec. 8, 2005) (discussing failure to disseminate written notice of necessity to preserve documents). But see Orbit One, 271 F.R.D. at 441 (failure to issue a written litigation hold “does not necessarily constitute negligence”).

106. Chin, 685 F.3d at 162.


108. Id. at 473 n.67 (quoting Shira A. Scheindlin et al., Electronic Discovery and Digital Evidence: Cases and Materials 147-49 (2009)).


• **Describe the potential types and sources of the material to be preserved.** In addition to describing the substantive content that qualifies a record for preservation, a hold should describe the types and sources of material to be preserved. For example, a hold should direct recipients to preserve all relevant records in both paper and electronic form,\(^{111}\) including drafts and nonidentical copies.\(^{112}\) A hold should further discuss documents located outside of the office, including, for example, documents in offsite storage,\(^{113}\) home offices,\(^{114}\) home computers,\(^{115}\) or personal email accounts.\(^{116}\) Describing the likely sources of the material sought will aid custodians in thinking through what relevant material may be in their possession.

• **Identify the individuals or groups to whom the hold applies.** The best-written hold will not be effective unless it is provided to the right people,\(^{117}\) including the “key players.”\(^{118}\) Also note that separate holds may be needed for any third parties identified as custodians as a result of the possession, custody, or control analysis. This requirement will be discussed in more detail in Section 3.3.3, Identifying and Interviewing Custodians.

• **Provide instructions for preservation and/or collection.** Beyond simply telling custodians to preserve things, custodians must be told how to preserve things. The hold must make clear that routine deletion procedures must cease.\(^{119}\) To this end, the hold might instruct custodians to create folders to store preserved records and discuss the disabling of any janitorial functions, such as the automatic deletion of email.\(^{120}\) Similarly, the hold might provide that backup tapes be removed from any overwriting rotation,\(^{121}\) and that hard drives containing relevant material may

---


112. See Metro. Opera Ass’n, 212 F.R.D. at 181.


114. See Pension Comm., 685 F. Supp. 2d at 482 n.125 (party had duty to search employee’s files even though employee did not work at employer’s office); accord Discover Fin. Servs., Inc. v. Visa U.S.A., Inc., 2006 WL 3230157, at *1 (S.D.N.Y. No. 8, 2006) (discussing requirement that company search CEO’s home files).

115. See Koosharem Corp. v. Spec Personnel, LLC, 2008 WL 4458864 (D.S.C. Sept. 29, 2008) (requiring inspection of home computers when employees were not initially issued laptops and instead used home computers for work).

116. See Easton Sports, Inc. v. Warrior LaCrosse, Inc., 2006 WL 2811261, at *3-6 (E.D. Mich. Sept. 28, 2006) (sanctioning defendant when employee terminated his personal Yahoo! email account, which contained relevant work information, after the lawsuit was filed). Counsel should be increasingly aware of potential issues with such offline data. As one survey found, 16% of respondents admitted using their personal email to avoid corporate review and retention of their emails. See George Stamboulidis, Ona Wong, Alberto Rodriguez, Working From Home: An Employee’s Dream; A Litigator’s Nightmare, N.Y.L.J. (June 30, 2008). But see Matthew Enter., Inc. v. Chrysler Grp. LLC, 2015 WL 8482256 (N.D. Cal. Dec. 10, 2015) (party did not have possession, custody, or control over employees’ personal accounts, as they could not force employees to turn them over).

117. See In re Pradaxa Prods. Liab. Litig., 2013 WL 6486921, at *6 (court found the defendants took too narrow a view on identifying custodians for a “company-wide” litigation hold).

118. See Goodman, 632 F. Supp. 2d at 512 (“key players” to receive litigation hold include individuals likely to have relevant information); Consol. Aluminum Corp. v. Alcoa, Inc., 744 F.R.D. 335, 342 (M.D. La. 2006) (noting inadequacy of litigation hold issued to 11 employees when initial disclosures named 100 employees); Zubulake V, 229 F.R.D. at 424 (criticizing counsel for failure to provide litigation hold instructions to key player).

119. See Zubulake IV, 220 F.R.D. at 218 (a party “must suspend its routine document retention/destruction policy”).

120. See Surowiec, 790 F. Supp. 2d at 1006, 1007.

121. See Se. Mech., 2009 WL 2242395, at *3; see also Zubulake V, 229 F.R.D. at 424 (counsel criticized for failure to safeguard backup tapes).
not be recycled. These issues will be discussed more in Section 3.3.4, Preservation in Place vs. Preservation by Collection.

- **Inform recipients of their legal obligations and the potential penalties for noncompliance.**

- **Provide instructions for communicating about the legal hold.** The hold should tell the custodians to whom they may speak about the hold and how they should conduct that communication. For example, a hold might specify that custodians should speak only with designated members of the in-house counsel team and should mark emails on the subject as privileged and confidential.

  Additionally, the notice should include a mechanism for verifying receipt and review by the custodians to whom the hold is sent. This can be done using a variety of methods, including by emailing the hold with a read receipt applied, by requiring each custodian to confirm compliance using legal hold software, by requiring each custodian to confirm receipt and review by email or via voting buttons, by requiring each custodian to sign and return an acknowledgement form, or by acknowledgment during an interview.

122. See Medcorp, Inc. v. Pinpoint Techs., Inc., 2010 WL 2500301, at *3-6 (D. Colo. June 15, 2010) (party sanctioned when hard drives were inadvertently destroyed in the routine course of business); Cache, 244 F.R.D. at 629 (once a litigation hold is instituted, a party cannot continue a routine procedure of wiping and recycling hard drives).

123. See ABA Civil Discovery Standard 10 (Aug. 2004) (“the lawyer should inform the client of its duty to preserve potentially relevant documents in the client’s custody or control and of the possible consequences of failing to do so”).

124. See In re Prudential, 169 F.R.D. at 612 (noting failure in preservation notice to designate a primary contact for information about document preservation).
Practice Pointer: Be Careful How You Word a Legal Hold

Numerous cases highlight the importance of carefully crafting the legal hold, tailoring the language to the issues in the lawsuit. Courts viewing a legal hold through the lens of hindsight will likely try to find indications of a party’s reasoning based upon the wording of the legal hold. Holds that are too broad in scope may result in a litigant creating a duty to preserve that would not otherwise exist.

In one multidistrict products liability litigation, the court found that a party anticipated litigation, such that it had a duty to preserve information, based upon the specific wording of the legal hold. Although various isolated products cases against the defendant had been filed in the past as early as 2003, with additional cases filed in 2007 and 2008, it was not until 2010 that additional cases were consolidated in an MDL. The defendant argued that litigation was not anticipated until the MDL. While the court noted that prior isolated lawsuits would not necessarily lead a company to reasonably anticipate large-scale products liability litigation, the court held that the legal hold references to prior “company-wide” hold notices from 2007 and 2008 and the continued obligation to retain materials evidenced the duty to preserve information preceded the MDL. The court specifically noted that “the scope of preservation was established . . . in the document preservation notices.”

Similarly, the Western District of Louisiana held that a duty to preserve evidence in a later filed MDL was triggered by the “broad and sweeping” language in an earlier general products liability litigation hold. The defendant claimed that it did not reasonably anticipate bladder cancer litigation until 2011, when the first bladder cancer lawsuit was filed. The defendant argued it had only anticipated lawsuits related to liver injuries. Yet, the defendant had issued a general legal hold in 2002 requiring the preservation of “any and all documents that discuss, mention, or relate to [the drug at issue].” The hold went on to instruct individuals to “interpret this directive in its broadest sense to prevent the deletion or destruction of any recorded information and data relating in any way to [the drug].” The court found that “the reality of an instituted hold undercuts [defendant’s] arguments as to when they should or should not have instituted a litigation hold” and that the “clear and unambiguous language in no way limits itself to a specific malady, but rather, ties itself to the drug involved.” Thus, the duty to preserve arose in 2002 when the defendant chose to issue a “broad and sweeping” litigation hold.

Such cases highlight the need for parties issuing a legal hold to consider limiting the hold’s language with respect to specific types of claims or types of harm, specific groups of potential claimants, specific types of documents, specific time periods, and specific custodians.

3.3.3 Identifying and Interviewing Custodians

Once the duty to preserve arises, counsel must identify sources of discoverable information, such as key players or IT personnel. “Key players,” including anyone listed in the initial disclosures, must receive a

It is also important to think about the managers of noncustodial data sources that need to receive the legal hold notice. For example, managers of departmental records may need to be notified to suspend any record destruction cycles that might affect relevant records, and IT administrators will need to be notified to suspend any automated janitorial functions (e.g., automated deletion of email older than a specified age). Failure “to cease the deletion of email” or “to preserve backup tapes when they are the sole source of relevant information” can also support findings of spoliation.

Beyond simply identifying additional custodians, custodial interviews should also be used to gather information about the types of relevant records each custodian possesses and the sources from which such records can be obtained. For example, one custodian might maintain all of his records in paper files, while another may make extensive use of her assigned network share drive, while still another works outside the office using his home computer. Asking each potential custodian a planned series of questions about the data he or she has and the places where he or she keeps it will facilitate a preservation and collection process that is both efficient and complete.

In addition to speaking to individual custodians, IT personnel must also be interviewed to obtain an understanding of the enterprise’s computer systems. A determination should be made as to what systems are used, where information may be stored, and what document retention policies are in place. Inquiries as to whether IT personnel are aware of any data or databases that contain relevant information should also be made. Counsel should further ask how data is stored, whether the data is accessible or inaccessible, what the archival process for data is, what data is routinely retained, whether hardware

127. See Consol. Aluminum, 244 F.R.D. at 342; see also Goodman, 632 F. Supp. 2d at 512; Zubulake V, 229 F.R.D. at 424.
129. See Zubulake V, 229 F.R.D. at 433.
130. See Surowiec, 790 F. Supp. 2d at 1006, 1007.
132. Zubulake V, 229 F.R.D. at 424 (counsel criticized for failure to speak with key player to understand how she maintained her computer files), 429 (counsel misunderstood client’s use of word “archive,” thinking client meant backup tapes when in reality client was referring to active data on a hard drive), 432 (counsel should speak to key players “to understand how they stored information”), 436 (counsel must ascertain key player’s document management habits).
133. See Delaware Court of Chancery Guidelines for Preservation of Electronically Stored Information.
134. See Zubulake V, 229 F.R.D. at 432 (counsel must speak to IT personnel “who can explain system-wide backup procedures and the actual (as opposed to theoretical) implementation of the firm’s recycling policy”); In re Seroquel, 244 F.R.D. at 663.
is ever recycled or stored,\textsuperscript{138} and how backups are retained, rotated, or destroyed.\textsuperscript{139} Based upon such conversations, counsel may need to instruct IT personnel to keep data in an accessible form if relevant systems are going to be sunsetting.\textsuperscript{140}

Third parties that possess relevant information that could be deemed within a party's control should also receive a legal hold and be instructed to retain relevant information.\textsuperscript{141} Due to the privileged nature of the internal legal hold communication, however, a separate legal hold should be created and distributed to any third-party custodians identified in order to preserve the privilege of the internal legal hold.

3.3.4 Preservation in Place vs. Preservation by Collection

After communicating the preservation obligation to the relevant personnel, preservation of records must actually be implemented. There are many ways to fulfill this obligation. As the court stated in \textit{Zubulake IV}, because “there are many ways to manage electronic data, litigants are free to choose how this task is accomplished.”\textsuperscript{142} The most important thing is to make sure that the end result is “a complete set of relevant documents.”\textsuperscript{143}

One approach is preservation in place. Preservation in place involves instructing custodians about what records must be preserved and having the custodians preserve the records where they are normally kept. This is a low-cost option, but it places heavy reliance on each custodian to ensure that the records are preserved, which can be a risk.\textsuperscript{144}

At the opposite end of the spectrum is preservation by collection, which involves going to each custodian and collecting all potentially relevant data, just as would be done prior to review and production. This is a more costly option, but centralized preservation of a collected data set avoids the distributed risk associated with having each custodian preserve in place. This approach should likely be used when a relevant custodian is leaving a company.\textsuperscript{145} Similarly, if there is a reason to suspect that spoliation may occur, such as situations in which a custodian has been accused of wrongdoing, preservation by collection

\textsuperscript{138} See \textit{Cache}, 244 F.R.D. at 629 (recycling or expunging of computers when employees leave a company must cease once there was a duty to preserve information).

\textsuperscript{139} See \textit{Zubulake V}, 229 F.R.D. at 432; \textit{In re Seroquel}, 244 F.R.D. at 663.

\textsuperscript{140} See \textit{Quinby v. WestLB AG}, 245 F.R.D. 94 (S.D.N.Y. 2006) (while it was not spoliation to move data to an inaccessible state, “if a party creates its own burden or expense by converting into an inaccessible format data that it should have reasonably foreseen would be discoverable material at a time when it should have anticipated litigation, then it should not be entitled to shift the costs of restoring and searching the data”).

\textsuperscript{141} See \textit{In re NTL}, 244 F.R.D. at 195-97 (duty to preserve documents held by spin-off corporation, as documents were within party's control), 198 (noting failure of party to inform computer vendor of preservation obligations).

\textsuperscript{142} \textit{Zubulake IV}, 220 F.R.D. at 218.

\textsuperscript{143} Id.

\textsuperscript{144} See \textit{Pension Comm.}, 685 F. Supp. 2d at 473 (noting litigation hold was inadequate when “the directive places total reliance on the employee to search and select what that employee believed to be responsive records”); \textit{accord Cache}, 244 F.R.D. at 629 (taking issue with “direct[ing] employees to produce all relevant information, and then rel[y]ing upon those same employees to exercise their discretion in determining what specific information to save”); \textit{Nat’l Day Labor Organizing Network v. U.S. Immigration & Customs Enf’t Agency}, 877 F. Supp. 2d 87, 108 (S.D.N.Y. 2012) (noting most custodians cannot be trusted to run effective searches for information).

\textsuperscript{145} See \textit{generally Cache}, 244 F.R.D. at 629.
should be implemented. Various approaches to collection are discussed further in Chapter 5, Collection and Processing.

A variation on the preservation-by-collection method is the keyword search for preservation. Enterprises may choose to run queries across systems to preserve ESI hit by the search terms. The construction of appropriate search criteria will be of particular import if this method is selected.

Whatever method of preservation is chosen, electronic files should be preserved in their native formats. Custodians and those collecting data for preservation should avoid modifying metadata by opening, printing, copying, or forwarding files.

In between these two approaches is a range of options such as collecting key custodians’ information but allowing secondary or tertiary custodians to preserve information in place.

Any of these approaches may be suitable depending on the nature of the matter, the scope of the records needing preservation, the custodians involved, the technological systems involved, and other factors. When a duty to preserve arises, the full range of options should be considered to determine the appropriate approach for that matter.

### 3.3.5 Monitoring Compliance with a Legal Hold

Numerous cases make clear that simply sending out a litigation hold is insufficient. Beyond simply establishing and distributing the hold, “counsel must oversee compliance with the litigation hold, monitoring the party’s efforts to retain and produce the relevant documents.”

Like preservation itself, monitoring has no one correct form. As long as the goal of preserving a complete set of relevant records is achieved, the method is acceptable. That said, there are several useful steps that should be considered:

- Documenting the issuance of the litigation hold and subsequent reminders.
- Requiring recipients of a litigation hold to verify in writing that they have received, understand, and will comply with the hold.
- Periodically reissuing the written hold or requiring recertification of continued compliance with it by all those subject to it.
- Directly communicating with key custodians to confirm their compliance.
- If preservation in place is used, meeting periodically with key custodians to review what they are preserving for the matter and how they are maintaining it.

---

146. See Zubulake V, 229 F.R.D. at 432.
147. Id.
148. See Metro. Opera Ass’n, 212 F.R.D. at 227 (noting how party had no checklist or written record of what was done).
149. See Zubulake V, 229 F.R.D. at 433; In re NTL, 244 F.R.D. at 197-98.
150. See Zubulake V, 229 F.R.D. at 434.
• Following up with any key custodians who have stated that they do not have documents to be preserved.\textsuperscript{151}

• Visiting the office or offices where relevant information is located.\textsuperscript{152}

• Sampling the materials being preserved to look for gaps or for references to other materials that may require preservation.\textsuperscript{153}

• If term searches are employed, whether by individual custodians or by departmental custodians, documenting the searches used and sampling the results to measure the searches’ effectiveness.\textsuperscript{154}

• Verifying that any automatic deletion functions or routine destruction of records has been suspended.\textsuperscript{155}

• Checking to see that backup tapes required to be preserved are separated from other materials and stored in a safe place.\textsuperscript{156}

3.3.6 Reissuing the Litigation Hold

The litigation hold should be periodically reviewed and reissued so that new custodians are aware of the litigation and so that it keeps the information in the hold fresh in the minds of all relevant custodians.\textsuperscript{157} In addition, if any additional custodians of relevant information are identified after the initial litigation hold was issued, counsel should provide a copy of the initial litigation hold to the additional custodians. An updated litigation hold should also be issued if new issues or subject matters arise in the litigation\textsuperscript{158} or if the parties reach an agreement with the other side regarding preservation obligations.\textsuperscript{159}

\begin{itemize}
  \item \textsuperscript{151} See Pension Comm., 685 F. Supp. 2d at 485 (noting how counsel failed to follow up with key custodians after custodians said that they had no documents).
  \item \textsuperscript{152} See Metro. Opera Ass’n, 212 F.R.D. at 212; see also Pension Comm., 685 F. Supp. 2d at 473 n.68 (counsel should spot-check preservation efforts).
  \item \textsuperscript{153} See Pension Comm., 685 F. Supp. 2d at 473 n.68.
  \item \textsuperscript{154} Accord Victor Stanley, Inc. v. Creative Pipe, Inc., 250 F.R.D. 251, 257 (D. Md. 2008) (“[t]he only prudent way to test the reliability of the keyword search is to perform some appropriate sampling of the documents”); In re Seroquel, 244 F.R.D. at 662 (“Common sense dictates that sampling and other quality assurance techniques must be employed to meet requirements of completeness.”).
  \item \textsuperscript{155} Fed. R. Civ. P. 37 advisory committee’s note (2015) (“As under the current rule, the routine, good-faith operation of an electronic information system would be a relevant factor for the court to consider in evaluating whether a party failed to take reasonable steps to preserve lost information, although the prospect of litigation may call for reasonable steps to preserve information by intervening in that routine operation.”).
  \item \textsuperscript{156} See Zubulake V, 229 F.R.D. at 434.
  \item \textsuperscript{157} Id. at 433; see also in re NTL, 244 F.R.D. at 197-98 (custodians should be periodically reminded of their preservation obligations).
  \item \textsuperscript{158} See Chen v. LW Rest., Inc., 2011 WL 3420433, at *10 (E.D.N.Y. Aug. 3, 2011) (noting defendant should have instituted a specific litigation hold with respect to relevant flash drive when it was requested by plaintiffs and ordered produced by the court).
  \item \textsuperscript{159} See In re Seroquel, 244 F.R.D. at 656 (noting parties should confer early on about preservation); see also Fed. R. Civ. P. 26 advisory committee’s note (2006) (it is useful for parties to discuss preservation); Delaware Court of Chancery Guidelines for Preservation of Electronically Stored Information (noting parties should confer about preservation).
\end{itemize}
3.4 What Are the Consequences for Failure to Preserve?

Federal Rule of Civil Procedure 37(e) controls the sanctions available when a party fails to preserve ESI. The Rule, which became effective on December 1, 2015, governs not only proceedings filed after this date but also those proceedings pending at the time of its effectiveness unless application to an already pending proceeding would be unjust or impracticable.\(^{160}\) The Rule “forecloses reliance on inherent authority or state law to determine when certain measures should be used.”\(^{161}\)

Rule 37(e) states:

If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:

(1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or

(2) only upon finding that the party acted with the intent to deprive another party of the information’s use in the litigation may:

(A) presume that the lost information was unfavorable to the party;

(B) instruct the jury that it may or must presume the information was unfavorable to the party; or

(C) dismiss the action or enter a default judgment.

In sum, sanctions under the Rule will only apply if (1) a party had a duty to preserve information and failed to take reasonable steps to preserve; (2) the information was lost as a result of the failure to take reasonable steps; (3) the information could not be restored or replaced through additional discovery;\(^{162}\)

---

\(^{160}\) See CAT3, 164 F.Supp. 3d at 495-496 (citing 2015 U.S. Order 0017; 28 U.S.C. § 2074(a)); see also Brown Jordan Int’l, Inc. v. Carmicle, 2016 WL 815827, at *36 (S.D. Fla. Mar. 2, 2016). But see Stinson v. City of New York, 2016 WL 54684, at *5 n.5 (S.D.N.Y. Jan. 5, 2016) (noting that since briefing on issue was submitted prior to effective date, even if opinion was issued after effective date, it would not be just and practicable to apply new Rule).

\(^{161}\) Fed. R. Civ. P. 37 advisory committee’s note (2015); see also HCC Ins. Holdings, Inc. v. Flowers, 2017 WL 393732, at *4 (N.D. Ga. Jan. 30, 2017) (citing advisory committee note in finding rule forecloses reliance on inherent authority to address spoliation of ESI). Yet, some courts continue to discuss inherent authority when looking at sanctions available for spoliation. See CAT3, 164 F. Supp. 3d at 497 (discussing committee note but also stating that courts have certain implied powers to manage their own affairs, including the power to impose sanctions for bad faith spoliation of evidence). And, parties should be cognizant of the fact that different legal analyses may govern the spoliation of hard-copy or tangible information. See Best Payphones, Inc. v. City of New York, 2016 WL 792396, at *3 (E.D.N.Y. Feb. 26, 2016) (noting “separate legal analyses govern[] the spoliation of tangible evidence versus electronic evidence” in applying Rule 37 to spoliation claims for destruction of ESI and Second Circuit case law to spoliation claims for destruction of hard-copy documents); see also United States v. Safeco Ins. Co. of Am., 2016 WL 901608, at *7 n.3 (D. Idaho Mar. 9, 2016) (noting Rule 37(e) did not apply to destruction of handwritten documents).

\(^{162}\) See Living Color Enters., Inc. v. New Era Aquaculture, Ltd., 2016 WL 1105297, at *4-5 (S.D. Fla. Mar. 22, 2016) (before looking at Rule 37(e)(1) or (e)(2), court looked at preliminary spoliation questions of:

- Does the alleged spoliation involve ESI?
- Was the allegedly spoliated ESI evidence that should have been preserved?
and (4) the loss of the information was prejudicial. The Rule provides a uniform standard for the use of more severe sanctions only when a party intentionally destroys information.\(^ {163} \)

In determining whether a party failed to take reasonable steps to preserve information, a court must first consider whether the party had a duty to preserve information at all.\(^ {164} \) Whether the party should have known that the destroyed evidence would become relevant in the case should be considered in assessing whether a duty to preserve existed.\(^ {165} \)

Assuming a duty to preserve existed, the court must next consider whether the party took reasonable steps to preserve information that has been lost.\(^ {166} \) The advisory committee's notes make clear that "reasonable steps to preserve suffice; [the Rule] does not call for perfection."\(^ {167} \) In determining whether a party acted reasonably in preserving information, courts may examine the sophistication of the litigants, whether any loss was outside the party's control, and the costs of preservation.\(^ {168} \)

Information may not be "lost" if it exists elsewhere and has already been produced from other sources.\(^ {169} \) But, if a party failed to take reasonable steps to preserve information in anticipation of litigation and information was lost and not produced from other sources, the focus should be on whether information can be restored or replaced through additional discovery.\(^ {170} \) Any efforts to restore or replace lost information should be proportional.\(^ {171} \) If information can be restored or replaced, or is marginally relevant or duplicative, no further action should be taken.\(^ {172} \)

The Rule underscores the need for the loss of information to be prejudicial to the other side. Absent prejudice, sanctions are not available.\(^ {173} \) Prejudice must be proven and cannot be presumed unless there

---

- Was the allegedly spoliated ESI lost because a party failed to take reasonable steps to preserve it?
- Is the allegedly spoliated ESI evidence that cannot be restored or replaced through additional discovery?

noting that if the answer to any question was "No," the court need not proceed any further in a spoliation analysis; see also Accurso v. Infra-Red Servs., Inc., 169 F. Supp. 3d 612, 618-619 (E.D. Pa. Mar. 11, 2016) (refusing to grant negative inference absent evidence of destruction of evidence that cannot be obtained from other sources).


164. See Living Color, 2016 WL 1105297, at *1 (finding court must first determine whether party had a duty to preserve evidence).

165. See Marten Transp., Ltd v. Plattform Advert., Inc., 2016 WL 492743, at *7-10 (D. Kan. Feb. 8, 2016) (refusing to find duty to preserve Internet history from outset of suit when original claims alleged unauthorized use of trademark but did not include improper access to website until later); see also Fed. R. Civ. P. 37 advisory committee's note (2015) ("Often these events provide only limited information about that prospective litigation, however, so that the scope of information that should be preserved may remain uncertain. It is important not to be blinded to this reality by hindsight arising from familiarity with an action as it is actually filed.").

166. See Living Color, 2016 WL 1105297, at *4-5.


168. See id.

169. See Living Color, 2016 WL 1105297, at *4-6 (text messages existing in multiple locations and already provided to plaintiff were not "lost," while text messages that were not replaced were lost); accord Fed. R. Civ. P. 37 advisory committee's note (2015) ("It applies only when such information is lost. Because electronically stored information often exists in multiple locations, loss from one source may often be harmless when substitute information can be found elsewhere.").


172. See id.; see also Living Color, 2016 WL 1105297, at *5.

173. See Best Payphones, 2016 WL 792396, at *6 (when party negligently failed to preserve evidence but defendant was not prejudiced by the destruction, "there has been no spoliation . . . under Rule 37(e)"); Living Color, 2016 WL 1105297, at *5-6 (when missing text messages appeared to be unimportant and there was an "abundance of information . . . sufficient to
was an intent to deprive. If there is prejudice, the court must determine what sanction, if any, cures the prejudice.

Rejecting prior case law, severe measures of presuming lost evidence is unfavorable to the party who lost the information, permissible presumption or adverse inference jury instructions, and dismissal or default are reserved for those instances where a party acts with an intent to deprive another party of information. Thus, the most severe sanctions will not be given, absent intent to deprive the other side of relevant information. As the advisory committee’s notes state, “Care must be taken, however, to ensure that curative measures under subdivision (e)(1) do not have the effect of measures that are permitted under subdivision (e)(2) only on a finding of intent to deprive another party of the lost information’s use in the litigation. An example of an inappropriate (e)(1) measure might be an order striking pleadings related to, or precluding a party from offering any evidence in support of, the central or only claim or defense in the case.”

Yet, even when a party intentionally destroys relevant information, the drastic measures allowed under Rule 37(e)(2) are not mandatory. A court should order sanctions no greater than necessary to redress the spoliation.

For a more in-depth look at the potential sanctions imposed for spoliation of evidence, see Chapter 8, Spoliation and Electronic Discovery Sanctions.

meet the needs of plaintiff,” plaintiff was not prejudiced by failure of party to turn off automatic deletion of text messages).

174. See Brown Jordan, 2016 WL 815827, at *37 (when party destroyed information with intent to deprive, court would presume that the lost information was unfavorable to destroying party); see also Fed. R. Civ. P. 37 advisory committee’s note (2015) (“Subdivision (e)(2) does not include a requirement that the court find prejudice to the party deprived of the information. This is because the finding of intent required by the subdivision can support not only an inference that the lost information was unfavorable to the party intentionally destroyed it, but also an inference that the opposing party was prejudiced by the loss of information that would have favored its position. Subdivision (e)(2) does not require any further finding of prejudice.”).

175. See Fed. R. Civ. P. 37 advisory committee’s note (2015) (the Rule “rejects cases such as Residential Funding Corp. v. DeGeorge Financial Corp., 305 F.3d 99 (2d Cir. 2002), that authorize the giving of adverse-inference instructions on a finding of negligence or gross negligence”); see also Accurso, 169 F. Supp. 3d at 618-619 (refusing to grant a negative inference absent an intent to deprive access to information).

176. See Bry v. Frontenac, 2015 WL 9275661, at *11 n.7 (Dec. 18, 2015) (when ESI was taped over pursuant to a standard operating procedure, there was no evidence of intent to deprive the other party of information, such that remedies under Rule 37(e)(2) were not available); Living Color, 2016 WL 1105297, at *6 (when party regularly deleted messages in order to keep phone running and had activated setting on phone to automatically delete text messages after 30 days prior to litigation, court found defendant acted negligently without an intent to deprive plaintiff, such that Rule 37(e)(2) remedies were not allowed).


178. See CAT3, 164 F. Supp. 3d at 501-502 (when finding intentional spoliation, the court ordered the payment of costs and the preclusion of evidence because more severe sanctions were not mandatory and lesser measures would be sufficient to redress the loss); Ericksen v. Kaplan Higher Educ., LLC, 2016 WL 695789, at *1-2 (D. Md. Feb. 22, 2016) (court would order measures no greater than necessary to cure intentional spoliation in ordering preclusion of evidence but denying request for dismissal).

179. Fed. R. Civ. P. 37 advisory committee’s note (2015); see also CAT3, 164 F. Supp. 3d at 501-502 (lesser measures would be sufficient to redress the loss); Erickson, 2016 WL 695789, at *1-2 (same); accord HM Elecs., Inc. v. R.F. Techs., Inc., 2015 WL 4714908, at *30 (S.D. Cal. Aug. 7, 2015) (finding lesser sanctions would be insufficient even if new Rule 37 were in effect in ordering adverse inference for intentional destruction).
3.5 When Can Preservation Cease?

The proper handling of ESI at the conclusion of litigation is just as important as its proper handling during a case. Once the obligation to preserve information ceases to exist, such as when litigation is ultimately concluded,\(^{180}\) a notice releasing the litigation hold should be issued. Frequently, the normal, nonlitigation retention period for documents and data not specially held under a legal hold can expire during the life of a case. Failure to release a litigation hold increases storage costs for retaining records that should be disposed of in accordance with records retention policies. In addition, without due attention, documents and data collected for one case can become a whole new source of discovery in subsequent cases.\(^{181}\) The enterprise will be required to incur the costs of searching and reviewing documents it should no longer possess.\(^{182}\)

At the conclusion of a matter, the litigation team and the client should take the following actions:

- Evaluate the protective order and any return/destruction requirements.
- Return or destroy produced data from opposing and third parties, including co-counsel, experts, and eDiscovery vendors.
- Determine whether the client will make any data available for use in other cases (collection dataset or production dataset).
- Evaluate whether data and documents are subject to legal hold(s) for other matters.
- Set the appropriate time period and manner of preservation of the data, if any.
- Appropriately dispose of other collected, reviewed, and produced data.
- Distribute “end of matter” notices to all individual custodians and systems custodians who had been subject to the legal hold.
- Send a thank-you note of recognition to everyone who has been supportive, including outside vendors.

As in all phases of the process, the resulting decisions should be documented and made part of the master file.

---

180. See generally Philips Elec. N. Am. Corp. v. BC Tech., 2011 WL 677462, at *7 (D. Utah Feb. 16, 2011) (ordering that a party must cease the wiping of hard drives until the termination of litigation); Hickson v. U.S. Postal Serv., 2010 WL 5963378, at *1 (E.D. Tex. Nov. 10, 2010) (court signed stipulation for dismissal that included language that “[t]he Postal Service may lift its Litigation Hold on all preserved documents, tangible items, and electronically stored information, including but not limited to all email correspondence, that may be relevant to this case”). But see Liberman v. FedEx Ground Package Sys., Inc., 2011 WL 145474, at *3 (E.D.N.Y. Jan. 18, 2011) (when plaintiff dismissed claim against FedEx and FedEx subsequently destroyed documents, court found FedEx spoliated documents because “after the first case was voluntarily dismissed, FedEx should have known that the records may be relevant to future litigation”).

181. See Association for Information and Image Management Presentation, The Business Case for Records Management—How to get a real return on your investment, www.aiim.org (citing study finding between 20% and 92% of records reviewed in nine cases for DuPont between 1990 and 1994 were past the relevant retention period, leading to an extra review expense of more than $11 million).

Information Governance: Managing Digital Debris

October 01, 2015

AUTHORS
Tess Blair, Rahul Kapoor

The ever-increasing growth of data content combined with complex legal and regulatory obligations makes information governance a critical business issue for organizations. In fact, nearly 70% of data generated by a company has no legal or business value, according to a report published by Electronic Discovery Reference Model (EDRM), an organization dedicated to improving the electronic discovery process. To help organizations determine how to dispose of digital debris, EDRM has developed an Information Governance Reference Model (IGRM).

Defining and Identifying Digital Debris. Before implementing data-governance policies, organizations need to understand what data needs to be kept and what data has no legal or business value. The default method of keeping all data forever may ensure that an organization has all data required by various regulations. However, this method is expensive and unwieldy, particularly as data continues to proliferate at stunning rates. For example, the same email can typically be found in multiple places, such as on email servers, local and networked archives, on smartphones, in the cloud, and on disaster recovery tapes and drives. Other files—such as temporary work files duplicated in multiple locations, data stored on outdated technology and litigation copies—can slow system performance, increase litigation costs, and increase the risk of loss, theft, or breach of sensitive information.

The Information Governance Reference Model. The IGRM was developed to help organizations define an effective information governance strategy. At its core, the IGRM links the legal obligations and business utility of specific data to the stakeholders who create, consume, and manage that data. IGRM recognizes that information management should not be relegated only to IT teams. All creators and consumers of information in an organization must work together. To effectively implement IGRM and create a defensible data-disposal program, an organization must have effective leadership responsible for information governance, must implement policies and processes that link information to relevant stakeholders and must provide stakeholders with the technology and tools to implement the organization’s information governance policies and procedures.

Implementing the Information Governance Reference Model. A critical step in implementing an effective IGRM is assessing an organization’s existing information governance process. This assessment will help an organization identify weaknesses in its existing data management strategies. Based on the organization’s assessment, the responsibilities of information management can be divided among three key groups: business users; legal, risk, and regulatory departments; and IT
Designing and implementing an effective information governance program can result in a significant payoff by reducing an organization’s risks and costs relating to the storage and management of data.

Tags: Cloud, Privacy, Regulatory, Shared Services, Technology

Read more from Tech & Sourcing @ Morgan Lewis

Copyright © 2019 Morgan, Lewis & Bockius LLP. All rights reserved.
## 9.5 Potential Sources of Information

### Email
- **Microsoft Outlook - .pst**
  - Runs on Exchange servers
  - Local .pst files
- **Lotus Notes - .nsf**
  - Runs on Domino servers
  - Mostly resides on servers
  - Can be locally replicated

### Webmail
- Gmail, Yahoo! Mail, AOL, etc.
- Lives on hosted servers - ISP
- Office 365
- Cloud-based email and productivity suite hosted by Microsoft

### Servers
- Stored on network devices, such as file servers
- Usually the same kind of data files as found on a PC: unstructured data, such as Microsoft Word documents, Excel spreadsheets, and PowerPoint presentations
- Either shared or personal
- Some organizations have document-management systems

### Databases
- Also known as structured data
- Document storage and information archiving and manipulation
- Typically accessed by many users
- Information updated regularly
- Usually have reporting capability

### Hard drives
- **Personal computer hard drive- typically contains:**
  - Data files – Microsoft Office (Word, Excel, PowerPoint)
  - Locally stored email in .pst or .nsf files
  - System files – make the computer run and are generally not relevant in discovery
  - Internet cache files – auto downloads that help you surf the Web and house Web history, cookies, and temporary Internet files
  - Deleted files – many “deleted” files can still be retrieved from computer hard drives using forensic tools. While a user may think that a deleted file is gone, the computer simply marks the space occupied by the file as available. It does not delete the file; therefore, the file can be resorted fairly easily. The space where deleted files can be found is often referred to as “slack” or “unallocated” space.

### Other communication tools
- Instant messaging – transcripts may be stored on individual users’ machines or company servers depending on which tool is in use and how it is configured
- Blogs – online diaries
- Chat rooms – bulletin boards and online locations for users of common interest to communicate online
- Text messaging – typed messages sent via cell phone or PDA; not stored by service provider and typically limited storage on device
- Digital phone (VoIP) and voicemail – digital voicemail is ESI

### Social media
- Facebook
- Twitter
- LinkedIn
- Instagram
- Snapchat
- Countless other user-controlled websites and apps for communicating, journaling, and otherwise sharing personal information

### Mobile devices
- Smartphones
- BlackBerrys
- iPods, MP3 players
- Portable storage devices and media – CDs, thumb drives, portable hard drives

### Cloud
- Amazon Web Services, Microsoft Azure
- Salesforce
- Dropbox, Syncplicity, Google Drive, iCloud

### Other
- Backups
- Keycard access logs
- Security camera footage
- Photocopier hard drives
- Voice recordings from recorded phone lines
- Always ask the question, “Are there other sources we haven’t considered?”

---

*Morgan Lewis eData Deskbook Third Edition*
When Must E-mails Be Produced in DGCL Section 220 Books and Records Actions?

By Michael D. Blanchard

- As technological advances have expanded the range of media used to conduct business, the law has also evolved regarding access to e-mail, text messages, and other forms of communication as books and records of the corporation.
- Although still evolving, some general principles have emerged that generally guide when the Delaware courts will permit access to electronic communications in section 220 proceedings.
- Producing e-mails in a books and records case cannot always be avoided, but there are steps corporations can take to mitigate the risk.

Since common law, stockholders have enjoyed a qualified right to inspect the corporation’s “books and records” for any “proper purpose”—i.e., a purpose reasonably related to the stockholder’s interests as a stockholder. Codified in state corporation statutes such as section 220 of the Delaware General Corporations Law (DGCL), these stockholder inspection rights were exercised infrequently until the Delaware courts began to encourage stockholders to utilize these “tools at hand” to obtain information necessary to plead demand excusal in derivative actions. As the Delaware Supreme Court noted in the seminal decision of Rales v. Blasband: “Surprisingly, little use has been made of section 220 as an information-gathering tool in the derivative context.” 634 A.2d 927, 935 n.10 (Del. 1993). Over the last 20 years, “Delaware courts have encouraged stockholders to use the ‘tools at hand’ (e.g., Section 220) to gather information before filing complaints that will be subject to heightened pleading standards.” Lavin v. West Corp., 2017 WL 6728702, at *9 (Del. Ch. Dec. 29, 2017). The significant increase in section 220 litigation over the last decade is a testament to the plaintiffs’ bar heeding the Delaware courts’ admonitions.

At the same time that section 220 books and records demands have become commonplace, rapid technological advances have driven the proliferation of the forms of media in which corporate information is kept, including, for instance, e-mails, text messages, and other electronic communications and records not traditionally viewed as a corporation’s “books and records.” The issue is only further complicated by the fact that officers’ and directors’ use of personal computers, smartphones, and personal e-mail accounts potentially renders communications beyond the direct control of the corporations whom the officers and directors serve. Until relatively recently, Delaware courts have been hesitant to compel the production of such “nontraditional” books and records in section 220 litigation, given that the extant jurisprudence dictates that a section 220 summary proceeding is far from coextensive in scope with Rule 34 discovery, and a stockholder is only entitled to those books and records deemed “necessary and essential” to achieving a proper purpose. Typically, board minutes, resolutions, and the like are deemed sufficient because the courts are mindful that a stockholder’s inspection rights must be balanced against the potential for burdensome and abusive “fishing expeditions” that mirror discovery requests in plenary corporate litigation. Nonetheless, as technological advances have expanded the range of media used to conduct business, the law has also evolved regarding access to e-mail, text messages, and other forms of communication as books and records.
records of the corporation. Although still evolving, some general principles have emerged that generally guide when the Delaware courts will permit access to electronic communications in section 220 proceedings.

Who cares? Corporations and their officers and directors absolutely should. Section 220 demands have become virtually a necessary prerequisite to any stockholder derivative action, and the books and records that stockholders receive and use to draft their complaint can be outcome-determinative on a motion to dismiss. Whereas board minutes and more “formal” corporate records will allow little room for “creative interpretation” by the plaintiffs’ bar, the same cannot be said of e-mail communications where plans and decisions are informally deliberated in real time, perhaps satirically or within a context that may not be evident when portrayed with hindsight by counsel whose objective is to prove a breach of fiduciary duty. Although producing e-mails in a books and records case cannot always be avoided, there are steps corporations can take on a clear day to mitigate the risk.

The seminal decision granting access to e-mails is a 2013 nonpublished transcript ruling, Ind. Elec. Workers Pension Tr. Fund IBEW v. Wal–Mart Stores, Inc., 7779–CS, at 97–98 (Del. Ch. May 20, 2013) (Strine, C.), which ironically does not directly address the issue of whether e-mails are corporate records subject to section 220 inspection rights. In Wal-Mart, then-Chancellor Strine ordered the production of private communications between officers and directors concerning an alleged bribery scandal under investigation by the plaintiff. In the process, the issue arose as to whether e-mails and electronic documents created or maintained on personal devices were the appropriate subject of a section 220 demand. The court drew no distinctions between e-mails and documents created by employees upon their personal devices verses those generated within the company’s official systems, concluding that where the documents were created or maintained was not controlling: “In terms of this issue of the home devices . . . if you use your home computer to handle Wal-Mart information, I don't think that many companies would believe that . . . that makes it their personal information.” Given that the e-mails were deemed corporate records necessary for the plaintiff to conduct its investigation, they were to be produced irrespective of where they were physically created or maintained. Although the unpublished Wal-Mart decision did not directly address when the production of e-mails is appropriate in a section 220 action, its affirmance on appeal was routinely cited by the plaintiffs’ bar for that principle.

The issue arose again in Chammas v. Navlink, Inc., 2016 WL 767714 (Del.Ch. 2016), a case involving a director’s demand for books and records pursuant to the more expansive rights that directors have as compared to stockholders. In Chammas, the director plaintiff sought to “investigate whether ‘the other members of the Board and management are excluding them from board business and related communications,’ including emails prior to Board meetings and alleged Secret Meetings.” Consistent with Wal-Mart, Vice Chancellor Noble first observed that whether a document or communication is stored on the company’s servers is “not necessarily determinative of whether it constitutes a book or record of the company.” More important, the court concluded, is whether the book or record must be “in the possession or control of the corporation.” Second, recognizing the importance of burden considerations in the section 220 context, the court disclaimed that although its “holding is not to be interpreted as a blanket prohibition against inspection of private communications among directors, subjecting Section
220 proceedings to such broad requests, even by directors, runs contrary to the ‘summary nature of a Section 220 proceeding.’” Finally, the court observed that the books and records of the company are “those that affect the corporation’s rights, duties, and obligations . . . .” The court’s ultimate rejection of the demand for e-mails turned on the insufficiency of the plaintiff’s evidence of wrongdoing to warrant their production: “Mere suspicions of pre-meeting collusion among board members or board members and management, in the context of a Section 220 action, is insufficient to compel the production of private communications between such officers and directors . . . .”

The same year Chammas was decided, Vice Chancellor Laster analyzed whether e-mails may be within the scope of books and records obtainable pursuant to section 220. In Amalgamated Bank v. Yahoo! Inc., 132 A.3d 752 (Del. Ch. 2016), a stockholder sought to investigate the hiring of Yahoo’s chief operating officer, and in that connection sought e-mails from the company’s CEO. The court began its analysis by categorically rejecting the argument that e-mails are per se beyond section 220’s scope. Vice Chancellor Laster observed the evolution of corporate record-keeping and the modern reality that virtually all books and records are now kept electronically: “Limiting ‘books and records’ to physical documents ‘could cause Section 220 to become obsolete or ineffective.’” The court then relied upon Wal-Mart to reject the argument that the company’s search for documents would be limited to the company’s devices, as opposed to a custodian’s personal device, holding that “a corporate record retains its character regardless of the medium used to create it.” As for the test to determine whether e-mails must be produced, the court limited itself to a single consideration: “As with other categories of documents subject to production under Section 220, what matters is whether the record is essential and sufficient to satisfy the stockholder's proper purpose, not its source.”

A few years later in Schnatter v. Papa John’s International, Inc., 2019 WL 194634 (Del. Ch. 2019), Chancellor Bouchard addressed the test suggested in Chammas as to whether e-mails (or any documents) are deemed books and records of the company—i.e., whether they are “those that affect the corporation’s rights, duties, and obligations . . . .” The defendant in Papa John’s resisted production of e-mails between directors discussing former director Schnatter, citing Chammas and claiming that “Schnatter is just curious about what his fellow fiduciaries were saying about him.” The court rejected the argument because the scope of documents ordered to be produced would be limited to those related to the plaintiff’s proper purpose, thus satisfying the standard. Commenting further, Chancellor Bouchard then effectively agreed with Vice Chancellor Laster’s reasoning for producing e-mails as articulated in Yahoo, albeit qualified by consideration of the additional costs inherent in producing electronic communications:

A further word is in order regarding emails and text messages from personal accounts and devices. The reality of today’s world is that people communicate in many more ways than ever before, aided by technological advances that are convenient and efficient to use. Although some methods of communication (e.g., text messages) present greater challenges for collection and review than others, and thus may impose more expense on the company to produce, the utility of Section 220 as a means of investigating mismanagement would be undermined if the court categorically were to rule out the need to produce communications in these formats.
Citing then-Chancellor Strine’s decision in Wal-mart, the court held that “if the custodians identified here . . . used personal accounts and devices to communicate about changing the Company’s relationship with Schnatter, they should expect to provide that information to the Company.” Expressly disclaiming the promulgation of any bright-line rule, Chancellor Bouchard grounded the analysis in “balanc[ing] the need for the information sought against the burdens of production and the availability of the information from other sources, as the statute contemplates.”

If there were any question about whether e-mails are properly within the scope of section 220 demands, the Delaware Supreme Court resolved it in KT4 Partners LLC v. Palantir Technologies Inc., 203 A.3d 738 (Del. 2018). In Palantir, after a potential sale of the company fell through because Palantir allegedly thwarted the deal and KT$ sought information pursuant to its far-reaching rights under an “Investors Rights Agreement,” Palantir allegedly amended the agreement to curtail KT4’s rights. KT4 made a demand to inspect Palantir’s books and records under section 220 of the DGCL for the purpose of investigating “fraud, mismanagement, abuse and breach of fiduciary duty.” Palantir rejected the demand, and KT4 commenced a section 220 action in the Delaware Court of Chancery. Following trial, Vice Chancellor Sights held that KT4 had shown a proper purpose of investigating potential wrongdoing in multiple areas, including Palantir’s amendment of the Investors’ Rights Agreement in ways that “eviscerated” KT4’s contractual information rights after KT4 sought to exercise those rights. The court specifically held that KT4 was entitled to “all books and records relating to” the amendments to the Investors’ Rights Agreement. After the parties were unable to agree on whether the books and records to be produced were to include e-mails, the court issued a final order that excluded e-mails from the documents that Palantir would be required to produce. The court reasoned in part that e-mails were not essential to fulfill KT4’s stated investigative purpose, based on the (mistaken) understanding that Palantir possessed and would produce formal board-level documents relating to the amendments of the Investors’ Rights Agreement, rendering a further production of e-mail unnecessary for KT4’s purpose.

KT4 appealed the Court of Chancery’s ruling. Importantly, on appeal, Palantir conceded that other than the amendments to the Investors’ Rights Agreement themselves, responsive nonemail documents did not exist, and that e-mails related to the amendments did exist. The Delaware Supreme Court held that the e-mails plaintiff sought were necessary and essential to investigating the alleged wrongdoing because the defendant admitted other, more traditional forms of books and records did not exist. Insofar as being required to produce e-mails was concerned, the Supreme Court viewed Palantir’s obligation as a self-inflicted wound. As the Supreme Court made clear, “if a company observes traditional formalities, such as documenting its actions through board minutes, resolutions and official letters, it will likely be able to satisfy a Section 220 petitioner’s needs solely by producing those books and records.” The court conversely cautioned that “if a respondent in a § 220 action conducts formal corporate business without documenting its actions in minutes and board resolutions or other formal means, but maintains its records of the key communications only in emails, the respondent has no one to blame but itself for making the production of those emails necessary.”

* * *

C:\Users\MP018018\Desktop\kt4.docx
The foregoing cases illustrate several principles inherent in any analysis of whether electronic communications will be ordered produced in section 220 litigation. First, electronic communications are deemed corporate records that may be ordered in section 220 proceedings, but only to the extent that they are “necessary and essential” to the plaintiff’s investigation. Second, whether or not the electronic communications reside on the corporation’s servers or personal devices, if they are necessary and essential to the plaintiff’s investigation, they may subject to an order compelling production. Third, although e-mails may be ordered to be produced in section 220 litigation, the cost and burden of such a production will weigh considerably in the court’s final determination. And finally, Palantir serves as an admonition to corporate boards and their counsel to be mindful to observe corporate formalities and appropriately document board meetings and actions through minutes, resolutions, and other official materials, and avoid conducting “formal corporate business . . . through informal electronic communications.” Absent proper recordkeeping and formal documentation of the board’s decisions, there is risk that a corporate respondent in a section 220 action may be ordered to produce e-mails as “necessary and essential” to satisfying a stockholder’s books and records demand.

Mr. Blanchard is a partner at Morgan, Lewis & Bockius LLP. He represents clients in all facets of shareholder litigation, class actions, securities enforcement matters, investigations, and business disputes. The views expressed by the author are his alone and are not the views of Morgan Lewis or the firms’ clients. This article is for information purposes only and does not constitute legal advice.