Chapter 2

Information Management Policies and Procedures

Kim Leffert & Michael Bornhorst

§ 2:1 Introduction

Information management policies and procedures are an important part of managing the risks and costs associated with electronically stored information (ESI). As organizations struggle with vast amounts of ESI and changing technology, particularly in connection with their legal and regulatory obligations to preserve, maintain, collect, and produce such ESI, cost-effective solutions are evolving to accommodate the developing law as well as advances in technology that alter the way the organization conducts its business. This chapter focuses on methods to meet these challenges through information management policies and procedures, particularly as they relate to the challenges of electronic discovery in the context of litigations, investigations, and requests for documents.

First, this chapter addresses two steps that an organization can undertake well before the initiation of the legal hold: (1) the preparation of an internal witness who has all information about the organization's data systems and who can testify about such systems at a deposition or explain those systems to opposing counsel or a regulator at a meet and confer; and (2) the preparation of a data source catalog, which is a guide for counsel to key data systems that often are subject to legal holds.

Next, this chapter addresses the key components of information management policies and procedures involving (1) email management; and (2) disaster recovery data management. These policies have proven to be of particular importance in the context of litigation and investigations; in a number of high-profile matters, the failure to properly manage data has led to its inadvertent destruction and has resulted in severe sanctions.

Having adequate knowledge of data systems and proper methods of managing ESI does not address an area of growing concern for organizations—the "legacy" data that is no longer needed for business reasons, but that has accumulated, and continues to accumulate, because of the risks associated with discarding any information given the legal and regulatory environment in which many organizations find themselves. This chapter outlines several approaches to the process of managing or remediating legacy data.

Finally, this chapter addresses some emerging trends in information management policies and procedures that may help organizations plan for future challenges.

§ 2:2 Managing Data Systems to Anticipate Litigation

§ 2:2.1 Internal Witness Preparation

As part of the process of furnishing information to litigants or regulators, organizations are increasingly required to provide specific information about their technology infrastructure and the steps they have taken to preserve and collect relevant information in response to the request (or complaint or commencement of investigation). Given the heightened importance of this information (which often is a strategic asset in negotiations about a case or other discovery issues), the information is often provided in some type of sworn statement, response to interrogatories, or a deposition of a company representative under Rule 30(b)(6) of the Federal Rules of Civil Procedure.

The best practice, as discussed in chapter 5, is to discuss and resolve any issues regarding the nature and scope of the relevant technology without the need for sworn statements, depositions, or hearings. However, if more formal discovery is required,[1] it is useful to create a list of potential questions that may arise in Rule 30(b)(6) depositions or electronic discovery hearings concerning the steps taken to comply with electronic discovery obligations in a particular matter. It is prudent to review these areas with the potential deponent, with careful attention to confirm the accuracy of all information regarding information technology procedures and electronic discovery processes that may be provided in the deposition or electronic discovery hearings. Many of these questions also can be used offensively, as an outline to depose an opposing party, as well as a means to collect information for the meet and confer.

While the preparation to respond to all of these questions may seem excessive, an organization involved in litigation or regulatory investigation is best served by having the comprehensive answers to all of them, to effectively address any issues in the discovery process, including management of associated costs. Indeed, ignorance (whether willful or inadvertent) of an organization's information management systems and the steps needed to preserve relevant information within those systems is a leading cause of discovery disputes, sanctions motions, and spiraling discovery costs.

---

1. Generally, an organization should consider resisting a deposition to obtain this type of information, as it is inefficient and costly and almost inevitably leads to further discovery, as well as running the risk of unintentionally impeaching other witnesses or submissions.

[A] Questions About Email Storage

The deponent may be questioned about

- email servers, including the number and location of servers;
- what operating systems are used for the email servers and if and when they have ever been upgraded;
- what software (that is, brand, version) is used for email; and
- email functionality, including how email is transmitted and whether there are prohibitions on user access to private email services (for example, AOL, Comcast, Google).

For Microsoft Outlook users, the deponent may be questioned about the Calendar, Contacts, To-do Lists and other features.

One of the key issues in any such examination will relate to the storage capacity for email, procedures for archiving email, deletion of email, tiered storage, and the like.[2] The deponent may be asked about

- whether and how copies of a user's mailbox are saved to the server or locally on the user's hard drive;
- whether a user can export or save email to any location on a file server;
- if and where a user can archive email and where else email could be stored;
- if it is possible that an email might not be stored anywhere (for example, user receives email but deletes it before a backup occurs);
- email storage limitations;
- groups or individuals with knowledge of or responsibility for policy or support in this area;
- email backup;
- whether users can search their local email using keywords and whether local mailboxes can be accessed from a central location by IT administration;
- whether users' incoming and outgoing emails are tracked or journaled, and if so, what tracking and journaling utility is used;
- email upgrades or retirement;

---

2. *See generally* The Sedona Conference WG1, *The Sedona Conference Commentary on E-mail Management: Guidelines for the Selection of Retention Policy*, 8 SEDONA CONF. J. 239 (2007).

- whether any automatic purges are used for email and whether and for how long a user-deleted email is recoverable from the server;
- what happens when a user's mailbox exceeds the size limit; and
- what happens to an employee's mailbox when the employee departs the organization.

[B] Questions About Laptops

The deponent may also be questioned extensively about the treatment of laptops of current and former employees and the treatment of the information on the hard drives during and after departure from employment (see also below). Thus, the questions may cover

- laptop hardware specifications, including make and model information and storage capacities;
- which operating systems the laptops use and if, when, and how they have been upgraded;
- which brands and versions of laptop software are used, including current and previous document management software, templates, and applications;
- whether employees can independently download nonapproved software to their laptop hard drives;
- which users are provided with a laptop and whether they can choose between a laptop and a desktop;
- whether the employer owns or leases the laptops it provides to users;
- the user file naming conventions (that is, how a user's portion of the file server is identified);
- user passwords for accessing the network;
- written policies or procedures regarding employee usage of the laptops and to identify groups or individuals with knowledge of or responsibility for policy or support in this area;
- whether files can be saved directly to the desktop or, instead, must be saved within an enterprise-wide document management program or network storage system;
- if and how laptop data is backed up;
- whether a user can search all files on a laptop using keywords and whether a laptop hard drive can be centrally accessed by IT administration;

- how laptops are upgraded or retired;
- if laptop hard drives are ever "wiped" and which software is used to wipe;
- what happens to a laptop when an employee leaves the organization;
- whether employees' hard drives are ever imaged, under what circumstances, and what types of images are created; and
- if and where an index of imaged hard drives is maintained, and if hard drives have been imaged in connection with the matter in question.

[C] Questions About Desktops

The deponent may be questioned about

- desktop hardware specifications, including make and model information and storage capacities;
- which operating systems the desktops use and if, when, and how they have been upgraded;
- which brands and versions of desktop software are used, including current and previous document management software, templates, and applications;
- whether employees can independently download nonapproved software to their desktop hard drives;
- which users are provided with a desktop and whether they can choose between a laptop and a desktop;
- whether the employer owns or leases the desktops it provides to users;
- the user filing naming conventions (that is, how a user's portion of the file server is identified);
- user passwords for accessing the network;
- written policies or procedures regarding employee usage of the desktops and to identify groups or individuals with knowledge of or responsibility for policy or support in this area;
- whether files can be saved be directly to the desktop or, instead, must be saved within an enterprise-wide document management program or network storage system;
- if and how desktop data is backed up;

- whether a user can search all files on a desktop using keywords and whether a desktop hard drive can be centrally accessed by IT administration;
- how desktops are upgraded or retired;
- if desktop hard drives are ever erased and which software is used to erase;
- what happens to a desktop when an employee leaves the organization;
- whether employees hard drives are ever imaged, under what circumstances, and what types of images are created; and
- if and where an index of imaged hard drives is maintained, and if hard drives have been imaged in connection with the matter in question.

[D] Questions About Procedures for Retaining Data for Departing Employees

In many cases, the key custodians may include former employees. In those cases, the deponent will be asked

- what happens to employees' laptops and desktops when they leave, for example, whether they are reissued to new employees or if and how their hard drives are wiped;
- whether hard drives of departing employees are ever imaged, under what circumstances, and what types of images are created;
- if and where an index of imaged hard drives is maintained, and if hard drives have been imaged in connection with the matter in question;
- if and for how long the emails of departing are retained; and
- what happens to an employee's BlackBerry device, PDA, or other handheld device when the employee leaves, that is, whether these devices are reissued to other employees and whether and how they are wiped prior to reissue.

[E] Questions About Records Management and Document Retention Policies

The deponent may be asked about (and typically should be able to furnish copies of) records management policies and procedures, including specific questions concerning

- whether there is a records management or document retention policy, and if so, what it is called; and

- whether the document retention policy explicitly covers electronic records, and if not, to identify any records retention policy for electronic records.

Furthermore, the deponent may be asked

- to describe the records management policy, document retention policy, or retention policy for electronic records;
- to describe the retention schedules under the policy, including general and specific schedules for potentially relevant data;
- to describe all retention plans and policies which apply to email;
- whether there is an automatic deletion function or limit on the time emails are retained;
- if such auto-deletion functions apply to all email folders or just specific ones (for example, inbox, sent mail, deleted mail);
- to describe any process available to provide for exceptions to such an auto-delete function;
- if there are time limits on the retention of email that is not the subject of auto-delete, and how these time limits are enforced;
- whether any of the time limits or auto-delete functions can be suspended;
- whether deleted items can be recovered in the email system, and if so, what period of time for deleted-item recovery is in use;
- if departed employees' email accounts are retained, for how long, who has access to them, and what procedures are followed to preserve or dispose of the data;
- if there is any scheduled deletion of accounts that were suspended;
- to describe all plans and policies regarding the retention and destruction of database information, including procedures and schedules for deletion of data and packing of the database files;
- to describe all plans and procedures for data retention on network systems, including time limitations on file storage and disk capacity limitations for users;
- whether there are any auto-delete or cleanup functions that were turned off;
- whether there are any scheduled deletions for user accounts (such as those of former employees) that were turned off;

- whether any of the procedures for the destruction or deletion of data, including data on document management systems, could be suspended pending litigation and, if so, if and when the procedure was suspended;
- to describe the destruction process for expired records, specifically electronic records and whether this process is centrally managed or managed by each department;
- whether expired records are reviewed by any corporate department (for example, legal or tax) prior to destruction; and
- if the destruction process is consistent for paper and electronic records.

[F] Questions About Home Computers

The deponent may be asked

- if there are any employees with desktop computers for home use, and if so, under what circumstances;
- if the organization policy permits, prohibits, or otherwise addresses employee use of computers not owned or controlled by the organization to create, receive, store, or send work-related documents or communications;
- about remote access to a computer network;
- which groups or individuals have knowledge of or responsibility for policy or support in this area; and
- about tracking information regarding home computers (for example, number, model, location).

[G] Questions About Portable Media

The deponent may be questioned about the policies and procedures which cover

- authorized or informal use of various portable media, including DVDs, USB flash drives, floppy drives, .zip drives, and any other standard portable media devices used;
- the identification of groups or individuals with knowledge of or responsibility for policy or support in this area; and
- the steps taken to preserve and collect relevant data from portable media.

[H] Questions About Handheld Devices

Increasingly, the less formal means of communication are the focus of questioning. Thus, the deponent may be asked about

- hardware and software used for smartphones, PDAs, BlackBerry devices, tablets, cell phones, or other handheld devices;
- which users are provided with a smartphone, PDA, BlackBerry device, tablet, etc., or, instead;
- organizational support for the use of such devices, including written policies and procedures, groups or individuals with knowledge of or responsibility for policy or support in this area, and synchronization with systems;
- whether the organization has what is often referred to as a "Bring Your Own Device" (BYOD) or "Bring Your Own Phone" (BYOP) policy, and if so, the scope of that policy;
- whether handheld devices are included in the organization's records management policies;
- whether handheld devices are included in litigation hold notices;
- whether data contained on such devices is backed up, and if so, whether it is backed up to the email server or a separate server;
- tracking information (for example, number, model, location) for these devices;
- what happens to these devices once the employee to whom they were issued leaves; and
- what steps were taken to preserve and collect relevant data from these devices.

[I] Questions About Internet and Intranet Usage and Social Media

The deponent should be prepared to respond to questions about

- whether the organization utilizes any Internet service providers for Internet or intranet access or maintenance of its Internet or intranet use, and about any limitations on Internet or intranet usage;
- utilization of any software or hardware programs or documentation as part of providing Internet or intranet access to its employees;

- any Internet- or intranet-related data maintained on the organization's systems, such as saved web pages, site listings, URL addresses, web browser software, bookmarks, favorites, cookies, or other folders;
- maintenance of records tracking employees' use of the Internet or an intranet; and
- any written policies and procedures, or groups or individuals with knowledge of or responsibility for policy or support in this area.

The deponent may also be questioned about social media. The questions may cover

- whether social media data will be collected as part of a compliance program or the discovery process in a litigation;
- whether social media is included in the records management policies;
- whether social media is included in litigation hold notices;
- where social media data may be captured (likely not in a structured database);
- whether data such as mobile phone data such as text messaging or GPS data are included;
- whether social networking sites, such as Facebook, LinkedIn, or Twitter are included;
- whether unstructured data is captured, such as audio, video, unstructured text (email text), or word processing documents;
- whether social media data are captured in the standard archiving processes;
- whether social media can be obtained through data snapshots of hard drives, such as forensic imaging of a hard drive;
- whether social media can be captured on a company server, on archives;
- whether social media can be obtained from active web pages or other social media users;
- the scope of the data;
- cost estimates for accessing the data;
- the best methods for obtaining the data;
- whether the organization has its own social media policy;

- how compliance with a social media policy is monitored; and
- whether request will be made for data on personal mobile devices or home computers (in which case, access would likely require court intervention).[3]

[J] Questions About Web Meetings and Collaboration Tools

The deponent may be asked

- if the organization utilizes any web meetings or other collaboration tools, and if so, which ones;
- if the organization saves the seminar presentations or minutes resulting from these meetings; and
- about any written policies and procedures, or groups or individuals with knowledge of or responsibility for policy or support in this area.

[K] Questions About Backup Systems

The deponent may be asked about the types of backup systems in place for the various types of data sources which have been identified as potentially relevant. Thus, questions may cover

- which hardware is used for backup and what the rotation schedule for backup tapes or other backup systems is, including any required by regulatory authorities;
- whether organizational policy calls for overwriting, reformatting, erasing, or otherwise destroying the content of the backups of network, email, or other servers on a periodic basis, and if so, what the rotation period is (if the rotation period has changed in the past ten years, the deponent should describe the changes);
- whether any of the procedures to overwrite, reformat, erase, or otherwise destroy the content of backup tapes can be suspended pending litigation, and if so, if and when the procedure was suspended;
- tape-labeling conventions and how and where tapes not currently in use are stored;

---

3. *See generally* The Sedona Conference WG1, The Sedona Primer on Social Media (Dec. 2012) (public comment version).

- any written policies and procedures or groups or individuals with knowledge of or responsibility for policy or support in this area; and
- whether, as a matter of organizational policy, employees' desktop and laptop hard drives are backed up in any way, and if so, under what circumstances and for how long are the backups retained.

The deponent should be prepared to discuss

- whether backup tapes are removed from rotation for any purpose, and if so, for what purpose;
- whether the organization possesses any backup tapes not currently used in active rotation; and
- whether the organization maintains an index of backup tapes that have been pulled from rotation and where such tapes are stored.

In addition, the deponent may be asked

- if the organization has ever restored any backup tapes, and if so, whether the restoration was successful; and
- to describe the restoration process (for example, labor, hours, equipment, devices).

The deponent may also be asked

- to describe the use of backup tapes, including the frequency with which each server is backed up (for example, daily, weekly, or monthly);
- whether each backup is incremental or a full backup;
- if the organization maintains at least one complete (nonincremental) backup of each server (network, email, etc.) for each month in the past ten years, and if not, for which months there exists a complete backup; and
- whether there is an incremental backup or other backups from which a full backup can be created of all data as of a given date for those months for which there is not a complete backup, and if so, describe the nature of such incremental or other backups and identify the months for which they exist.

Finally, the deponent may be asked if archival backups are created, and if so, what files have been archived.

[L] Questions About Preservation

Depending upon the scope of the topics identified, and the extent to which the attorney work-product or attorney-client privilege may apply, the deponent should be prepared to

- describe all steps taken to preserve electronic information in connection with the litigation;
- describe how preservation notices are implemented, communicated, and enforced and how any follow-up efforts after the initial preservation notice are communicated;
- provide a list of all the employees to whom the notice was sent and a description of the documents or categories of documents to be preserved;
- describe how backup holds are implemented, communicated, and enforced;
- describe how any follow-up efforts after the initial retention hold or backup hold are communicated; and
- provide copies of all hold notices sent to the corporate IT and records management departments, any outsourcing organization involved with electronic data, and any third parties that may store organization electronic data, including the date of the notice and list of employees or other persons to whom the notice was sent.

An increasingly important aspect of these depositions is the impact of features which automatically delete or overwrite information.[4] The deponent should be prepared to discuss whether

- auto-delete or similar program functions are in routine use, and whether they have been turned off, and if so, when (if not, the deponent should explain which functions have not been turned off and why); and
- if steps have been put into place to avoid deletion or modification of shared data, including department and project network shared data, group mailboxes, and public folders or discussion databases, and if so, when (if not, the deponent should explain which shared data is not so protected and why).

The deponent may be asked if steps have been put into place to cease the rotation of appropriate backup tapes, and if so, which backup systems and which tapes have been preserved, and if not, why.

---

4. *See* FED. R. CIV. P. 37(f) advisory committee notes (2006).

The deponent may also be asked

- if the organization has imaged hard drives of key persons and persons leaving the organization, and if so, what systems or programs were used to prepare the images;
- which computer hard drives were imaged and when;
- if the organization has searched hard drives that were imaged in connection with other matters for data related to key persons in this action;
- what software or other tools has the organization used to search for potentially relevant electronic records;
- if preserved documents are being stored in a central repository or other central place, and to describe its location and format (for example, a dedicated server);
- whether the party stores potentially relevant information with third-party service providers (in the "cloud"), and, if so, what steps the party has taken to identify, preserve and access the data; and
- to provide a record of all document preservation efforts performed, including a description of the effort and the date performed.

[M] Questions About Collection

The deponent may be asked to

- describe all steps taken to identify and retrieve potentially discoverable electronic data;
- identify all persons who supervised and carried out such efforts, describing each person's role;
- specify which computers, hard drives, backup tapes, third-party storage facilities for ESI, servers, and other storage media were searched for potentially discoverable electronic data;
- describe the types of data (for example, files, email, databases) that were searched;
- specify whether any deleted data was retrieved and if so, describe such data;
- describe the procedures and software used to search for and copy potentially discoverable electronic data; and
- provide a record of all collection efforts performed, including a description of the effort, copies of any questionnaires, surveys,

or interview summaries regarding employees' records, a log of the persons from whom documents were collected, a list of the persons from whom documents were not collected and the reasons, and the date each act was performed.

[N] Questions About Group (Shared) Network Drives

The deponent may be questioned about group or shared drives. The questions may cover

- what saving a document to the network server means for the organization or its departments;
- whether employees have a dedicated place on a network server to save files they create or receive (that is, a personal network drive);
- whether the personal network drive is in addition to or in place of the individual user's local, desktop hard drive;
- how and when files are backed up;
- to what extent files are accessible remotely;
- whether files are accessible to parties other than individual users (for example, assistants, other personnel);
- whether, in order to share documents, individual users must email files to requesting parties;
- similarly, whether employees, departments, etc. that routinely share documents have their own "shared" network drives;
- what parties have access to system administrator rights and how may these access rights be granted or removed as necessary over time (for example, for new hires, departures, or transfers);
- whether the organization utilizes a document management program, such as PC Docs® or WorldDox®;
- whether distinctions exist between personal and shared network drives (levels of access; differences in purge policies; drives spaces allocated to each);
- how to identify relevant shared drives in the context of a litigation;
- whether drives are no longer in use (for example, for former employees); and

- what drives were accessed by potentially relevant personnel over the life of an employee or group.[5]

[O] Questions About Structured Databases

The deponent may be questioned about structured databases. The questions may cover

- what databases exist within the organization;
- the form of the ESI;
- how the database is used in the ordinary course of business;
- what software applications are used to store database information;
- for each database, (1) what is the discrete information stored; (2) within each set of discrete information, what are the data elements (also known as fields) or data records stored; and (3) what is the common format and repository, such as a database or field-delimited data file;
- whether structured databases are used in unexpected contexts, such as email archives or websites;
- individual database rules for how information can be entered, stored, and retrieved;
- how to access key information, whether a single data field or reports that extract information from multiple tables;
- whether there is a system for distinguishing relevant database information from irrelevant information;
- how to collect and produce database information (for example, by field names, field codes and values, input constraints, or auto-filled fields);
- how database information may be used by the requesting party in a litigation and how to manage risk;
- how to run queries on database information; and
- whether there is database information in a third party's custody or control.[6]

---

5. Seth E. Pierce, *Navigating the E-Discovery Maze: What Every Litigator Should Know*, law.lexisnexis.com.
6. *See generally* The Sedona Conference WG1, *The Sedona Conference Database Principles: Addressing the Preservation & Production of Databases & Database Information in Civil Litigation* (2011).

§ 2:2.2 Data Source Catalogs

As part of an effective information management program, a data source catalog containing fact sheets on key data sources likely to be relevant across multiple litigations and investigations should be prepared. There may be a core, or common set, of applications typically involved in the routine cases, and more specialized systems and applications which need to be analyzed for more complex matters.

A careful, updated catalog, prepared in cooperation with the IT department, will facilitate discussions about preservation and collection decisions for key data sources without the need to repeat the investigative process in each litigation or investigation.

A data source catalog could include the following categories, depending upon the nature and use of the application at issue:

Data source: The name of the source should be identified in a way that is comprehensible to the owner of the data source as well as counsel (in-house and outside).

Business area: The name of the primary business unit or functional department that utilizes the data source should be identified to help counsel understand whether the data source may be relevant to the investigation or litigation. Units or departments that have potential access to the information should also be indicated.

Key contacts: The name and contact information (phone number or email address) of the person(s) responsible for maintaining data in the source should be identified. This will allow counsel to quickly contact a knowledgeable person about any questions relating to preservation or production from the source, including date range and type of data maintained.

Key functionality: The main functions of the data source should be described in pithy terms. This information helps explain why the data is maintained and what business purpose the source serves.

Brief description: A brief description of the type of data that is stored in the data source (for example, email, spreadsheets, financial data, personnel files, etc.). This assists counsel in understanding and explaining to outside parties what data is being maintained in the data source.

Inputs: Data sources, if any, from which data in the source is being pulled should be identified. Identifying inputs helps explain the actual source of the data, which is useful if there is a need to retrieve additional data from the original source, or where the original source may be a better source for the data.

Outputs: A description of the normal destination of information when transferred should be included. Identifying outputs helps explain where the data also may be stored, and in what form, which is useful because there may be a need to retrieve additional data from those destination data sources, or those destination data sources may be a better source for the data.

Date range and retention policy: The date range represented by the data stored in the source should be identified, as well as the retention policy for that data. This information helps counsel understand and explain to outside parties what data is being maintained in the data source, including how far back data may be kept in the data source.

Backup schedule: The schedule for any backups of the data source should be identified, including when the source is backed up and what type of backup is performed (that is, incremental or full). Identifying a backup schedule helps counsel understand and explain to outside parties how the data source is being backed up, if at all, which may inform preservation efforts for that data source.

Retention period for backups: The retention policy, if established, for any backups should be identified (that is, how long each backup is retained). Where no policy is in effect or the actual practice deviates from policy, careful notes should be made of the variances. Identifying a retention policy and the actual period of retention for backups of data sources helps counsel understand and explain to outside parties what data is being maintained in the backups for that data source, which may be important in relation to preservation efforts.

Preservation considerations: How is data preserved in this source? Is data preserved indefinitely? If so, what is the process for doing so (for example, snapshot of the source, export data that needs to be preserved, functionality in the source that allows for indefinite preservation)? What are the unique burdens and costs associated with preservation? Answering these questions about preservation of data in a data source helps counsel understand and explain to outside parties what steps can be, or were, taken to preserve data that is relevant in a matter; if preservation of data is particularly burdensome or costly; or if the source owner has a preferred method for preservation. It also may assist in making decisions about whether to assert that the information source is inaccessible.

Production considerations: How often is data from this source produced in a litigation or investigation? What is the standard output for production (for example, Excel spreadsheet)? What is the turnaround time to produce data from this source? Have there

been any modifications to the current source from the off-the-shelf source that may effect production and review? What are the costs and burdens of producing data from this source? Answering these questions about production of data from a data source helps counsel understand and explain to outside parties what steps can be, or were, taken to produce data from this data source that is relevant in a matter; if production of data is particularly burdensome or costly; or if the source owner has a preferred method for production.

Scheduled upgrades: Any information about scheduled upgrades to the data source should be identified, including when upgrades are scheduled to start, how long they will take, whether all the data will be migrated, and if migrated, whether the data will undergo any modifications. In light of this information, outside parties can be notified, if appropriate, and counsel can provide any necessary legal guidance.

Legacy data sources: If the information is not in active use, or cannot be readily accessed or retrieved from existing software or a centralized location, all relevant information about the legacy data source should be identified, including the timing of any previous access; whether and how the data was migrated into the new data source, and whether duplicative or essentially identical data exists, including the historical data from which the source was created. This information helps counsel understand and explain to outside parties what sources were being used during the relevant time and whether the data still exists in the same format.

§ 2:3 Records Management Policy

§ 2:3.1 Email and Other Communication

Electronic mail (email) has become critically important within the corporate setting and has been the subject of competing views on policy issues, especially about the length of time that a user maintains access to the information.[7] Many organizations are trying to cope with the mass increase in email use, while facing competing business, regulatory, and litigation requirements imposed on email.[8] As of 2008,

---

7. *See* The Sedona Conference WG1, *The Sedona Conference Commentary on Email Management: Guidelines for the Selection of Retention Policy*, 8 SEDONA CONF. J. 239 (2007); *The Sedona Principles: Best Practices Recommendations and Principles for Addressing Electronic Document Production* (The Sedona Conference Working Group Series, 2d ed. 2007), www.thesedonaconference.org.
8. The Sedona Conference WG1, *The Sedona Conference Commentary on Email Management: Guidelines for the Selection of Retention Policy*,

it was reported that less than half of entities in the United States and the United Kingdom have any clear strategy or policy in place to deal with ESI in litigation or investigations.[9] This may be changing, however as one survey of companies noted more than 65% of the companies planned to implement new email retention policies in 2008.[10]

Many problems encountered in identifying, preserving, and producing email communications could be avoided or alleviated by purchasing software or hardware. An important general issue, discussed below in section 2:5.2, is whether courts will compel or encourage parties to invest in such technology—perhaps by declining to shift costs if the investment is not made. For example, magnetic backup media (for example, backup tapes) are already being eclipsed by newer, far more accessible technology, such as disks.[11] This development raises the question whether there should be universal use of extended or archival storage of communications. Some courts profess not to understand why this approach is not routine in the business world. In *ClearOne Communications v. Chiang*,[12] the court criticized an email system that did not retain copies of email sent by a party. The court described this as "a significant irregularity; almost unimaginable for a technology company; and even more unlikely for a person of [the party's] importance in such a company."[13]

---

8 SEDONA CONF. J. 239 (2007). *See also* The Sedona Conference WG1, *The Sedona Conference Commentary on Information Governance* (Public Comment Version, Dec. 2013).

9. News Release, Kroll Ontrack, *Business Leaders Face Severe Risk from Lack of Ownership of ESI Policies* (Dec. 10, 2007) (reporting on a survey showing that 43% of respondents in the United States and 48% in the United Kingdom have a policy), https://www.businesswire.com/news/home/20071212005018/en/Business-Leaders-Face-Severe-Risk-Lack-Ownership.

10. *See* News Release, MessageOne, *New Survey Finds Over Half of Businesses Lack a Clear Email Retention Policy* (Dec. 17, 2007) (quoting Osterman Research; noting the "vastly different approaches to email retention" in place).

11. *See* Shamus McGillicuddy, *Law Firm Finds Tape Unreliable, Switches to Disk* (Sept. 24, 2007), http://searchcio.techtarget.com/news/1272977/Law-firm-finds-tape-unreliable-switches-to-disk.

12. ClearOne Commc'ns v. Chiang, No. 2:07 CV 37 TC, 2008 WL 704228 (D. Utah Mar. 10, 2008).

13. *Id*. at *1. The court held that since no evidence existed that it was done in bad faith, each party could argue that no one knows the entire contents of the sent email at trial. *Id*. at *4. *See* Northington v. H&M Int'l, No. 08 C 6297, 2011 WL 662727 (N.D. Ill. Feb. 14, 2011) (finding that defendant's efforts to preserve evidence had been reckless and grossly negligent, and requiring that defense counsel conduct a thorough search for ESI and hard copy and that the jury be instructed regarding defendant's failure to preserve).

Obviously, other types of communications need to be considered as well.[14] Instant messaging functions, both authorized and unauthorized, VoIP,[15] and other newer technologies will present challenges for corporate policy similar to those presented by email.

Even entities that have developed and maintained policies and procedures for managing different kinds of communications must be aware of the need to keep them updated. As the Court of Federal Claims noted while sanctioning the United States for failure to adequately preserve email, "antiquated and inadequate" retention and preservation policies can contribute to the problem.[16]

The Sedona Conference offers four key guidelines for determining an email retention policy.[17] The guidelines are suitable for public and private entities alike.[18] As an initial matter, any email retention policy should be reasonable, both in purpose and as applied, while also ensuring compliance with any applicable statutory and regulatory mandates that may directly or indirectly govern email management.[19]

---

14. George Paul & Jason Baron, *Information Inflation: Can the Legal System Adapt?*, 13 RICH. J.L. & TECH. 10, ¶ 21 (2007), http://law.richmond.edu/jolt/v13i3/article10.pdf (referencing instant messaging, word processing with hyperlinks, integrated voice mail in ".wav" file format, structured databases of all kinds, Web pages, blogs, and e-data in all conceivable forms). *See* McClain v. Norfolk S. Ry. Co., No. 3:07CV2389, 2009 WL 701001 (N.D. Ohio Mar. 16, 2009) (cell phone photographs).
15. Voice over Internet Protocol. For requirements on producing text messaging data, see City of Ontario v. Quon, 560 U.S. 746 (2010). The Court reversed the Ninth's Circuit's ruling that the City of Ontario, California violated the Fourth Amendment rights of one its police officers by searching and reading the personal text messages contained on the city-owned pager issued to the officer. While expressly declining to decide whether the officer had a protected Fourth Amendment interest in his text messages, the Court held that the search conducted by the City was not unreasonable because it was motivated by a legitimate government interest and was reasonable in time and in scope.
16. United Med. Supply Co. v. United States, 77 Fed. Cl. 257, 274 & n.30 (Fed. Cl. 2007) (noting the failure to take into account the applicable statute of limitations on retention periods and the "*ad hoc*" manner of notifying facilities involved). For evolving standards regarding production of metadata, see Nat'l Day Laborer Org. Network v. U.S. Immigration & Customs Enf't Agency, No. 10 Civ 3488(SAS), 2011 WL 381625 (S.D.N.Y. Feb. 7, 2011) (opinion and order withdrawn per order from court June 7, 2011) (finding, in Freedom of Information Act (FOIA) action, that certain metadata is an integral or intrinsic part of an electronic record and, as such, is readily reproducible in the FOIA context).
17. The Sedona Conference WG1, *The Sedona Conference Commentary on Email Management: Guidelines for the Selection of Retention Policy*, 8 SEDONA CONF. J. 239, 239 (2007).
18. *Id*.
19. *Id*. at 240.

Under the first guideline, email retention policies should use a team approach to reflect the input of functional and business units and should also include the entire organization, including any operations outside the United States.[20] The ideal would be an interdisciplinary team designed to assess the entity's email retention policy, comprised of representatives of legal, IT, records management, compliance, finance, and other major business units, both national and international. Team members should use the expertise of consultants, outside lawyers, and vendor representatives. A leader should be appointed to help the team reach its implementation goals.

Second, the team should "develop a current understanding of email retention policies and practices actually in use within the entity."[21] The goal should be "to identify the practical gaps, if any, between existing retention policies and actual practices,"[22] including the costs and risks involved in each. This analysis can aid in proposing changes to the existing policy.

Third, entities should "select features for updates or revisions of [the] email retention policy with the understanding that a variety of possible approaches reflecting size, complexity and policy priorities are possible."[23] In practice, the unique experiences of the entity within the legal, regulatory, and business contexts will govern the types of choices available. Team discussion can begin by analyzing the preferred duration of continued email access for users. Reaching a consensus on all points may prove difficult, but team members should be encouraged to openly discuss their differing points of view. An attempt should be made to compare the policies of similarly sized organizations to see what they have found useful.[24]

Finally, "[a]ny technical solutions should meet the functional requirements identified as part of policy development and should be carefully integrated into existing systems."[25] As a cautionary note, "[a] revised email retention policy may require the purchase or licensing of additional software and/or hardware to expand storage capacity. . . ." Any assessment of the suitability of such products should be driven by business, technical, and records management considerations.[26]

It is clear, however, that where discovery obligations are in direct conflict with specific business practices involving email or any other form of communication, the former trumps the latter, even where

---

20. *Id*. at 243.
21. *Id*.
22. *Id*.
23. *Id*. at 244.
24. *Id*.
25. *Id*. at 246.
26. *Id*.

destruction of information would otherwise be mandated by regulation or internal policy. As pointed out in *Renda Marine, Inc. v. United States*,[27] "a records retention policy which is inconsistent with a party's obligations to a potential or actual adversary in litigation [does not] excuse the party's failure to respond to discovery."[28]

§ 2:3.2 Disaster Recovery Data

"Disaster recovery data" is information preserved for use in the event of an emergency—for example, a natural disaster or a cyber attack—that damages or destroys an organization's primary data retention system. Because disaster recovery data is often kept in a format that is difficult and expensive to access,[29] such as backup tapes, courts have held that a party is generally not obligated to preserve disaster recovery data, "even when it reasonably anticipates litigation."[30] The 2006 amendments to the Federal Rules of Civil Procedure affirm this approach, stating that "[a] party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost."[31]

---

27. Renda Marine, Inc. v. United States, 58 Fed. Cl. 57 (Fed. Cl. 2003).
28. *Id*. at 61 n.4 (noting that compliance with the policy might bear on the issue of culpability, if sanctions sought, as federal law required a showing of "subjective bad faith"). For further discussion of bad faith, see Victor Stanley, Inc. v. Creative Pipe, Inc., 269 F.R.D. 497 (D. Md. 2010) (*Victor Stanley II*) (declining to order incarceration for defendant's bad faith spoliation, but ordering monetary sanctions of $337,796.37).
29. *See* 1 JAY E. GRENIG, ET AL., eDISCOVERY & DIGITAL EVIDENCE § 7:3 (2007) (disaster recovery data is "not normally organized for retrieval by date, author, addressee, or subject matter, and may be very costly and time-consuming to investigate thoroughly").
30. Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 217 (S.D.N.Y. 2003) (*Zubulake IV*) (citing *The Sedona Principles: Best Practices Recommendations and Principles for Addressing Electronic Document Discovery*, cmt. 6.h (Sedona Conference Working Group Series 2003)).
31. FED. R. CIV. P. 26(b)(2)(B). *See* FED. R. CIV. P. 26(b)(2) advisory committee notes on 2006 amendment ("[S]ome sources of electronically stored information can be accessed only with substantial burden and cost. In a particular case, these burdens and costs may make the information on such sources not reasonably accessible."); *The Sedona Principles*, *supra* note 7, cmt. 8.b ("Whether a source is 'reasonably accessible' does not solely depend on the technology required to access that information, but is more closely related to the costs and burdens involved in accessing and retrieving that information. The Advisory Committee gives, as [an example], 'backup tapes' intended for disaster recovery purposes. . . ."); Dilley v. Metro. Life Ins. Co., 256 F.R.D. 643, 645 (N.D. Cal. 2009) (granting a Rule 26(c) protective order where responding to an interrogatory request "would be overly burdensome" to defendants); SEC v. Collins & Aikman Corp., 256 F.R.D. 403, 410–11 (S.D.N.Y. 2009) (holding that

Because disaster recovery data is often considered "not reasonably accessible," it is generally exempt from production requirements.[32] However, Rule 26(b)(2)(B) specifies that courts have discretion to order the production of such data "if the requesting party shows good cause,"[33] and the advisory committee has stated that "[a] party's identification of sources of electronically stored information as not reasonably accessible does not relieve the party of its common-law or statutory duties to preserve the evidence."[34]

Using this formulation, many courts have applied preservation requirements, as implemented by a litigation hold process, to disaster recovery data, sanctioning parties which failed to prevent overwriting or reuse of the media, despite the associated burden and high costs.[35]

---

a "page-by-page manual review of ten million pages of records" constituted undue hardship on a defendant). However, where a backup tape is the sole source of information relevant to anticipated litigation, data should be preserved to avoid a finding that party was "grossly negligent" or a risk of an adverse inference. *See* Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC, 685 F. Supp. 2d 456, 471 (S.D.N.Y. 2010), *abrogated by* Chin v. Port Auth. of N.Y. & N.J., 685 F.3d 135 (2d Cir. 2012). *See also* Radian Asset Assurance, Inc. v. Coll. of Christian Bros. of N.M., No. CIV 09–0885 JB/DJS, 2010 WL 4928866 (D.N.M. Oct. 22, 2010) (finding that the burden and cost of production of backup tapes pursuant to an order of non-waiver should be shifted to plaintiff and upon finding the ESI not reasonably accessible, ordering backup tape production pursuant to an order under Rule 502(d)).

32. *See* Palgut v. City of Colorado Springs, No. 06-CV-01142, 2007 WL 4277564, at *3 (D. Colo. Dec. 3, 2007) (classifying defendant's backup tapes as "not currently accessible . . . since [defendant does] not have the hardware to access them" and noting that "the cost of restoration outweighs the possible yield of relevant and probative information"). *See also* Report of the Judicial Conference Committee on Rules of Practice and Procedure, at 30 (Sept. 2005), www.uscourts.gov/rules-policies/archives/committee-reports/reports-judicial-conference-september-2005 ("[A] party need not produce electronically stored information that is not reasonably accessible because of undue burden or cost. . . . [E]xamples under current technology include . . . information kept on some backup-tape systems for disaster recovery purposes.").

33. FED. R. CIV. P. 26(b)(2)(B).

34. FED. R. CIV. P. 26(b)(2)(B) advisory committee notes on 2006 amendment. *See also* Zubulake v. UBS Warburg LLC, 217 F.R.D. 309 (S.D.N.Y. 2003) (*Zubulake I*).

35. *See, e.g.*, Toussie v. County of Suffolk, No. 01-CV-6716, 2007 WL 4565160, at *8 (E.D.N.Y. Dec. 21, 2007) (characterizing defendant's failure to preserve backup tapes pursuant to litigation hold as "negligent," though declining to award spoliation sanctions); Semsroth v. City of Wichita, 239 F.R.D. 630, 632, 640 (D. Kan. 2006) (Acknowledging that "[t]he City keeps back-up tapes for disaster recovery purposes only," but holding that "the court cannot conclude that the cost . . . of restoring and

Therefore, it is recommended that an organization develop a comprehensive written policy dealing with the treatment of backup tapes or other disaster recovery data, considering the factors outlined below.

[A] Implementing a Retention Plan

Because "[t]he adoption and consistent compliance with a policy defining a preservation decision-making process is one factor that demonstrates reasonableness and good faith in meeting preservation obligations,"[36] an organization should develop a comprehensive written policy dealing with the treatment of disaster recovery data such as backup tapes or other forms of archived data.[37] Such a policy should provide "rational and defensible guidelines" for managing stored information, and should be created after considering the relevant business, regulatory, tax, information management, and infrastructure needs of the organization.[38]

The Eighth Circuit Court of Appeals in the seminal case of *Lewy v. Remington*[39] provided some useful guidance for determining whether the loss of information pursuant to a retention policy was appropriate under the circumstances:

- A retention policy should be reasonable considering the facts and circumstances of the documents in question.
- Courts may consider the frequency and magnitude of similar complaints against the organization, such that the organization should have known not to destroy relevant documents.

---

searching the . . . back-up tape . . . is such as to render that back-up tape 'not reasonably accessible because of undue burden or cost.'"); Consol. Aluminum Corp. v. Alcoa, Inc., 244 F.R.D. 335, 342 (M.D. La. 2006) (awarding costs where defendant "potentially spoiled relevant evidence through its failure to override its standard document destruction policies when this litigation became reasonably foreseeable"); Hous. Rights Ctr. v. Sterling, No. CV03-859 DSF, 2005 WL 3320739, at *3, *7 (C.D. Cal. Mar. 2, 2005) (counsel's failure to verify with client whether there was an email backup system "cannot be countenanced"; failure to search backup tapes owing to "honest miscommunication" between client and counsel as to existence of such tapes existed was at least grossly negligent).

36. *The Sedona Conference Commentary on Legal Holds: The Trigger and the Process* 8 (The Sedona Conference Working Group Series, Aug. 2007).

37. *The Sedona Principles, supra* note 7, cmt. 1.b.

38. *Id.*; Orbit One Commc'ns, Inc. v. Numerex Corp., 271 F.R.D. 429 (S.D.N.Y. 2010) (addressing defendant's motion for sanctions, the court found that although plaintiffs did not engage in model preservation of electronically stored information, they were not subject to sanctions absent evidence that any relevant information had actually been destroyed).

39. Lewy v. Remington Arms Co., 836 F.2d 1104, 1112 (8th Cir. 1988).

- Courts should evaluate whether the organization instituted the policy in bad faith.

[B] Consideration of Relevant Regulations

In addition to these general guidelines, an organization should take into account relevant laws or regulations requiring the preservation of certain types of data. Heavily regulated industries often face specialized rules governing the retention of electronic data.[40]

For example, members of national securities exchanges, brokers, and dealers are obligated to retain data under SEC regulations,[41] and publicly traded companies in the United States have data retention requirements under the Sarbanes-Oxley Act.[42] Therefore, while an organization's retention plan for disaster recovery data should be related to business policies, it should also be formulated with an eye toward any legal or regulatory provisions that may dictate the duration or scope of the preservation of disaster recovery data.

[C] Regular Recycling and Destruction

"Like the destruction of other ESI, the destruction of disaster recovery data" pursuant to a reasonable, good-faith retention policy where no litigation is anticipated is normally acceptable, as courts recognize that it would be unreasonable to require an organization to retain all possible relevant information.[43] Because retention policies tend to

---

40. *See, e.g.*, Byrnie v. Town of Cromwell, Bd. of Educ., 243 F.3d 93, 108–09 (2d Cir. 2001) ("Several courts have held that the destruction of evidence in violation of a regulation that requires its retention can give rise to an inference of spoliation."), *superseded in part by* Fed. R. Civ. P. 37(e).
41. *See, e.g.*, 17 C.F.R. § 240.17a-4 (SEC rule requiring members, brokers, and dealers to preserve certain records—including electronically stored records—for prescribed periods of time).
42. 18 U.S.C. § 1519 (Sarbanes-Oxley Act § 802) ("Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined under this title, imprisoned not more than 20 years, or both.").
43. *See, e.g.*, Arthur Andersen LLP v. United States, 544 U.S. 696, 704 (2005) ("'Document retention policies,' which are created in part to keep certain information from getting into the hands of others, including the Government, are common in business. It is, of course, not wrongful for a manager to instruct his employees to comply with a valid document retention policy under ordinary circumstances." (citations omitted)); *Zubulake IV, supra* note 30, at 217 ("Must a corporation, upon recognizing the threat of litigation, preserve every shred of paper, every email or

lower storage costs and reduce the burden of document retrieval in response to business requests, government investigations, or litigation, courts rarely impose sanctions where relevant documents were recycled or destroyed consistent with an organization's stated policy.[44] Without such a policy in place, however, the destruction of certain disaster recovery data might be seen by the courts as "selective," and viewed with suspicion, especially when only relevant documents are destroyed.[45]

The mere fact that policies are facially neutral does not exempt a party from suspicion as to motivation—but it helps when they are challenged.[46] In *Stevenson v. Union Pacific Railroad*,[47] for example, the Eighth Circuit, applying *Lewy*, held that while a party cannot rely on its routine document retention policy as a "shield" when the preservation duty attaches, "[w]here a routine document retention policy has been followed . . . there must be some indication of an intent to destroy the evidence for the purpose of obstructing or suppressing the truth in order to impose the sanction of an adverse inference instruction."[48]

[D] Dealing with Litigation Holds

As discussed above, the existence of an effective, written retention plan supports the argument that an organization has acted reasonably and in good faith in meeting its obligations with respect to preserving disaster recovery data. However, it is also important to

---

electronic document, and every backup tape? The answer is clearly, 'no'. Such a rule would cripple large corporations . . . that are almost always involved in litigation."); Forest Lab., Inc. v. Caraco Pharm. Lab., Ltd., No. 06-CV-13143, 2009 WL 998402, at *3 (E.D. Mich. Apr. 14, 2009) (refusing to grant relief for alleged spoliation of backup tapes where a producing party was "unaware of a need to safeguard evidence").

44. *See* 1 JAY E. GRENIG, ET AL., eDISCOVERY & DIGITAL EVIDENCE § 11:15 (2007).

45. *See id*.

46. *See, e.g.*, Wood v. Sempra Energy Trading Corp., No. 3:03-CV-986 (JCH), 2005 WL 3465845, at *8 (D. Conn. Dec. 9, 2005) (finding no violations of duty because defendant "froze any destruction that might have taken place in the ordinary course"); *see also* Broccoli v. Echostar Commc'ns Corp., 229 F.R.D. 506 (D. Md. 2005) (explaining duty to interrupt automatic deletion of email of key players once litigation hold applied).

47. Stevenson v. Union Pac. R.R., 354 F.3d 739 (8th Cir. 2004) (affirming prelitigation sanctions for failing to preserve voice tapes which were only contemporaneous evidence of conversations between train crew and dispatchers, but declining to sanction failure to prevent destruction of track maintenance records until after a demand was served for their production).

48. *Id*. at 747.

have procedures in place to put the regular recycling or destruction of disaster recovery data on hold.[49] When dealing with the prospect of a litigation hold, for instance, it might become necessary to suspend disaster recovery retention policies to insure that relevant evidence is not destroyed in the course of the routine destruction or recycling of backup tapes. The destruction of data, even if part of a clearly articulated data retention plan, can incur court-ordered discovery sanctions if the data was destroyed or lost at a time when a preservation obligation was in effect.[50] As the Eighth Circuit explained in *Lewy*:

> In cases where a document retention policy is instituted in order to limit damaging evidence available to potential plaintiffs, it may be proper to give an [adverse inference] instruction. . . . Similarly, *even if the court finds the policy to be reasonable given the nature of the documents subject to the policy, the court may find that under the particular circumstances certain documents should have been retained notwithstanding the policy*. For example, if the corporation knew or should have known that the documents would become material at some point in the future then such documents should have been preserved. Thus, a corporation cannot blindly destroy documents and expect to be shielded by a seemingly innocuous document retention policy.[51]

---

49. *See generally The Sedona Principles*, *supra* note 7, Principle 5 ("An organization's policies and procedures must mandate the suspension of ordinary destruction practices and procedures as necessary to comply with preservation obligations related to actual or reasonably anticipated litigation, government investigation or audit.").

50. *See, e.g.*, Pension Comm. of the Univ. of Montreal Pension Plan, *supra* note 31, at 465; Treppel v. Biovail Corp., 249 F.R.D. 111, 121 (S.D.N.Y. 2008) (holding that failure to preserve backup tapes was sufficient to constitute gross negligence or recklessness); Wingnut Films, Ltd. v. Katja Motion Pictures Corp., No. CV 05-1516-RSWL SHX, 2007 WL 2758571, at *13–21 (C.D. Cal. Sept. 18, 2007) (awarding sanctions for, among other things, defendant corporation's failure to suspend its automatic deletion of emails and other electronic documents as part of a litigation hold); Peskoff v. Faber, 244 F.R.D. 54, 60 (D.D.C. 2007) (quoting Disability Rights Council of Greater Wash. v. Wash. Metro. Transit Auth., 242 F.R.D. 139, 146 (D.D.C. 2007)) ("While . . . Rule 37 . . . indicates that, absent exceptional circumstances, a court may not impose sanctions on a party for 'failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system,' it is clear that this Rule does not exempt a party who fails to stop the operation of a system that is obliterating information that may be discoverable in litigation."). *Cf. Toussie*, *supra* note 35, at *8 (characterizing defendant's failure to preserve backup tapes containing information from the individuals sued as "negligent," though declining to award spoliation sanctions).

51. *Lewy*, *supra* note 39, at 1112 (emphasis added).

§ 2:3.3 Databases

As disputes over the discovery of ESI in data repositories, or databases, become increasingly common in civil litigation, the need to understand this vast information source grows. A database may be defined as follows: "In electronic records, a set of data elements, consisting of at least one file or of a group of integrated files, usually stored in one location and made available to several users."[52] Indeed, more organizational information is being stored in shared databases than in individual files. While this provides safeguards, such as the capacity to have files backed up, this protocol also adds to the burdens of electronic discovery when the information must be produced. Additionally, both requesting and producing parties must be aware of the information stores, even though company-wide information may vary, as may the attributes of databases. The size of systems may also dictate the methods of discovery used in data repositories, as some systems may encompass multiple servers, as opposed to less extensive databases. Similarly, archival databases that add new information without deleting past records also differ from transactional databases where data may be retained for short periods of time.[53]

In database discovery, information technology professionals may play a more integral role, advising attorneys about system structures in order to avoid "blunderbuss" requests, or requests for databases that typically encompass irrelevant or inappropriate information, including the production of terabytes of undifferentiated data.[54] Although the diversity of systems has made it difficult to develop best practices, the Sedona Conference's *Database Principles* provides six standards for developing effective and practical solutions in discovery of organizational information:

1. Absent a specific showing of need or relevance, a requesting party is entitled only to database fields that contain relevant information, not the entire database in which the information resides or the underlying database application or database engine.

2. Due to differences in the way that information is stored or programmed into a database, not all information in a database

---

52. The Sedona Conference WG1, *The Sedona Conference Glossary: E-Discovery and Digital Information Management (Third Edition)* 13 (2010).
53. The Sedona Conference WG1, *The Sedona Database Principles: Addressing the Preservation & Production of Databases & Database Information in Civil Litigation* ii–iii, 1 (2011).
54. *Id*. at ii.

may be equally accessible, and a party's request for such information must be analyzed for relevance and proportionality.

3. Requesting and responding parties should use empirical information, such as that generated from test queries and pilot projects, to ascertain the burden to produce information stored in databases and to reach consensus on the scope of discovery.

4. A responding party must use reasonable measures to validate ESI collected from database systems to ensure completeness and accuracy of the data acquisition.

5. Verifying information that has been correctly exported from a larger database or repository is a separate analysis from establishing the accuracy, authenticity, or admissibility of the substantive information contained within the data.

6. The way in which a requesting party intends to use database information is an important factor in determining an appropriate format of production.[55]

§ 2:3.4 Data Privacy

Data privacy issues are increasingly important, and organizations must consider a variety of related issues:

- how an organization's records management policy considers procedures that address the creation, identification, retention, retrieval, and ultimate disposition or destruction of information and records in compliance with data privacy;
- the scope of data, both technological and geographic (for example, whether covered data include instant messages, text messages, social media);
- how preservation and collection of data occurs;
- whether data is from the EU and therefore comes under more strict privacy laws;
- jurisdictional concerns due to cross-border discovery;
- how inconsistent data privacy regulations can be resolved;
- whether organization can employ devices to narrow the data set in order to alleviate privacy concerns;

55. *Id.*

- whether it is necessary to seek approval from local data privacy authorities to obtain permission to review and produce the ESI;
- whether redactions can alleviate data privacy concerns;
- whether internal information governance policies and procedures can be implemented both globally and locally, if necessary;
- how compliance with legal requirements can be monitored;
- how information technology; human resources; or marketing departments can facilitate compliance with data privacy laws;
- the interplay between data privacy policies and business policies regarding the use of facilities and equipment primarily;
- policies and procedures addressing the protection of trade secrets and commercial information may provide starting points for data privacy programs; and
- the applicability of statutes and regulations addressing privacy rights of individuals (such as the Health Insurance Portability and Accountability Act (HIPAA) of 1996).

Other countries often have fundamentally different restrictions under their local privacy laws. For example, in the European Union, the Charter of Fundamental Rights of the European Union recognizes that "each person has a right to the protection of personal data and that such data must be processed fairly, for specified purposes and on the basis of the consent of the person or some other legitimate lawful basis," including the fundamental right to access personal data and to correct any mistakes in that data.[56] And the European Union's recently enacted General Data Protection Regulation (GDPR), which applies both to organizations within the EU and those that do business inside the EU, imposes a number of data privacy protections upon organizations, including the so-called "right to be forgotten," allowing individuals to request that certain personal information

---

56. 2000/C364/01, Article 8. The legislation protecting individuals' rights in relation to personal data is mostly contained within Directive 95/46/EC on Data Protection (the "Directive"), which seeks to harmonize the applicable national legislation for each member state. The Directive applies to any data that identifies an individual, including name, address, telephone number or specific physical characteristics. The collection, storage, retrieval, transmission and destruction of data all fall within the definition of "processing" under the Directive. The majority of the obligations with respect to personal data fall on "data controllers," defined as those responsible for processing personal data.

be removed from an organization's data systems.[56.1] In contrast, in China, there is limited regulation on document retention, 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.[57]

§ 2:4 Remediation of Legacy Data

§ 2:4.1 Nature of Legacy Data

Large volumes of potentially relevant data often accumulate in locations or formats that are difficult and expensive to access, and the marginal value of production of such data is exceeded by the burdens and costs involved. Accordingly, many entities are considering steps to remediate or otherwise organize the information.

Legacy data that is appropriate for remediation typically includes:

- Data that is outside the organization's records management policies—that is, data that is not covered by those policies;
- Data that is not responsive to active or anticipated litigation holds—that is, data that has been preserved for some purpose but is not subject to an active litigation hold;[58] and
- Data that is not required for a present or anticipated business purpose—that is, data that has been preserved for some purpose and which presently serves no function or has no utility for the organization.

Generally, legacy data includes data that is not part of an organization's active systems, but which has been archived on various "offline" media, including hard drives, CDs, DVDs, and backup tapes. However, as discussed below, there are data sources on an organization's active system that fall outside a record retention policy, and are not being used in the ordinary business operations, such as obsolete applications or personal or home drives of departed employees, that may be inadvertently taking up costly storage space on the active systems (and likely increasing risks in investigations and litigations).

56.1. The EU's General Data Protection Regulation took effect in May 2018. Regulation 2016/679. The GDPR builds upon the Directive (discussed *supra* note 56), both by imposing additional obligations on "data controllers," and by increasing the territorial scope of the data protection obligations.

57. *The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age* 20, 37–38 (2004).

58. Data that is subject to a legal hold may be deemed appropriate for remediation if, after conducting extensive analysis, an organization determines that the data is duplicative of more accessible data.

The ultimate goal of a remediation project is to bring legacy data that is not subject to an active legal hold within the record retention policies of an organization, and to manage the risks associated with legacy data effectively.

§ 2:4.2 Costs and Risks Associated with Legacy Data

It is important to evaluate the costs and risks that result from the retention of legacy data. Typically its retention exposes an organization to significant risks, particularly where knowledge about legacy data sources is limited, and results in substantial costs, which often are hidden or not fully appreciated because they are dispersed across an organization in different departments or business units.

[A] Costs and Risks of Storage and Data Management

The continued retention of legacy data makes data management both riskier and more costly. Storing vast quantities of legacy data renders effective management unfeasible, and thereby increases the risk of mistakes stemming from the management of that data. It also results in increased costs of management—costs of both physical storage and personnel. The more geographically diverse the legacy data is (that is, the more it is dispersed across physical locations in the organization or at various off-site storage vendors), the more risk and cost is usually associated with it. And often the most "cost-effective" storage, such as a closet at a data center, carries the most risk (including the risk of data being "lost" or "inadvertently destroyed").

For example, proper retention of backup tapes or hard drives requires specific storage conditions to avoid the degradation of the storage media type, and the longer such media are stored, the more likely the degradation that corrupts the data becomes. Ideally, if proper retention is the goal, data should eventually be transferred to more effective long-term storage. In reality, what often leaves the legacy data source vulnerable to degradation is that no one wants to make a decision about remediation of the source, and no one is willing to incur any additional costs.

[B] Costs and Risks of Disclosure

The retention of legacy data subjects an organization to greater risks and increased costs of disclosure of confidential or other types of sensitive information that may reside in legacy data sources. The continual accretion of legacy data results in an increase in the risk of mistakes with respect to disclosures. That risk is increased where legacy data accumulates unbeknownst to counsel, or where counsel does not have enough knowledge about legacy data sources

to make accurate representations and disclosures in litigations and investigations. Indeed, without proper investigations into legacy data sources, both in-house and outside counsel risk a court or regulator determining that a "reasonable inquiry" was not made into sources of potentially relevant information. Thus, one who knows of a store of legacy backup tapes, or suspects that orphaned personal drives from departed employees may exist on an organization's active systems, and fails to make further inquiry, may risk sanctions. The subsequent destruction of such data, even if inadvertent, may also expose the organization to spoliation charges.

Conversely, the cost of employing counsel or paraprofessionals to search for and examine all potentially relevant data sources, including legacy data sources, in connection with an ongoing matter for disclosure requirements substantially increases the cost of litigation. Indeed, given the likely difficulty in determining what type of data may be located on a legacy data source, including the potential of expensive forensic work, it would be difficult to come to definitive conclusions in the course of an ongoing matter without excessive costs. Moreover, an organization must always weigh the risks of making data more "accessible" versus the risk of not having firm conclusions about what data is located on a legacy data source, and the weighing of such risks can be skewed in the context of a specific litigation or investigation.

[C] Costs and Risks of Production

The continued retention of legacy data subjects an organization to increased costs of production because, by definition, the data must be reviewed before production. The larger and more unwieldy the organization's store of legacy data, the more burdensome its production requirements are likely to be.

For example, in highly regulated industries it is becoming increasingly common for multiple copies of some individuals' data to be stored and archived. Email may automatically be archived (so that all email sent or received is saved in a separate archive), but email may also be archived by the individual on a hard drive or personal drive on the network. In the course of upgrades for laptops or desktops, copies of active files on hard drives may be preserved, and that same data may be copied and harvested from the hard drive for various investigations or litigations over the years. All of this data may be stored on backup tapes as well. In sum, vast amounts of accumulated data may be available for production for just one custodian. It could cost tens of thousands of dollars to process all of this custodian's accessible data, and even more for restoring data from less accessible sources such as backup tapes.

Moreover, with all this legacy data, it is more likely that discovery disputes will arise, and that outside counsel's contesting discovery requests for such information will add to the total costs of production.

§ 2:4.3 Remediation Prerequisites

Of course, implementing remediation plans presents various challenges, which relate to the volume of data, the form of the data, and the available tracking of that data. The prerequisites for a successful remediation project include:

- The organization has taken reasonable steps to identify and catalog its legacy data;
- The organization has a current records management program;
- The organization has an understanding of its litigation holds, including which holds are active and which holds may be released; and
- The organization has access to the underlying legacy data store and has access to facilities, tools, or vendors with the capability to analyze the data and assist with remediation of the data as appropriate.

§ 2:4.4 Measuring Success of Remediation

Measures of success for the remediation project can include the following:

[A] Litigation Holds Management System

The successful remediation project will result in the creation of a holds management system, which is a database that allows in-house counsel to effectively track legal holds by listing all relevant information about each legal hold including docket numbers (if appropriate), responsible in-house counsel, data range for the hold, a list of custodians, and a list of databases and other data sources subject to the legal hold.

In addition, the holds management system achieves the following objectives:

- Improved information quality for data maintained in the holds management system about legal holds, including an understanding of which litigation holds are active and what the scope of those holds is;
- Release of inactive litigation holds (and associated release of data maintained for those holds);

- Improved understanding of when litigation holds should be lifted going forward.

[B] Legacy Data Maintenance

With respect to legacy data maintenance, an organization should consider the following criteria in assessing the success of its program:

- Reasonable assurance that legacy data has been comprehensively identified and cataloged;
- Reasonable assurance that identified legacy data can be actively managed (including collecting in a central location, as appropriate);
- Integration of litigation hold status in the holds management system with the in-house counsel's evidence-tracking database;
- A significant amount of data appropriately remediated, including appropriately discarded or migrated to better platforms.

§ 2:4.5 Remediation of Different Types of Data

The remediation process entails categorizing the data and/or media type into appropriate categories. At the most basic level, data can be categorized as either centralized or noncentralized. As discussed below, the categorization of data will dictate how the remediation analysis will be performed for each media type, but generally data needs to be centralized in order to effectively remediate data without as much risk.

[A] Centralized Data

Centralized data generally is readily accessible, and is often gathered as a result of a legal hold, or maintained because of concerns identified by the legal department. Examples include inventories of backup tapes or images of hard drives.

For purposes of remediation, it is helpful to think of centralized data as divided into four categories: matter-specific, custodian-level, organizational-level, and media-level.

[A][1] Matter-Specific Data

Matter-specific data is data that can be readily identified by a category that relates to a substantive issue for an industry. For instance, in client-based industries, data that can be identified by client would be matter-specific: for example, information relating to client accounts in a financial institution, to an audit client in an accounting firm, or to a legal client in a law firm. In product-driven industries, such as pharmaceuticals or manufacturing, matter-specific data would be

product-specific data as data relating to research and development, marketing, and sales for a product. Generally, matter-specific data is the easiest type of data to remediate.

Organizing data in a matter-specific fashion clearly makes sense for many business purposes. But it also aids in the preservation and collection of data subject to legal holds, as the data is organized in a way that makes it more easily identifiable by counsel as being subject to a hold. Counsel also can quickly determine if matter-specific data can be remediated pursuant to normal record retention policies because no legal hold is applicable, and the records department can quickly identify what record retention policies apply to matter-specific data.

Generally, when commencing a remediation project, the ultimate goal will be to narrow the data to matter-specific data in order to limit the risk of lifting a hold, although that is not always necessary, as discussed below.

[A][2] Custodian-Level Data

Custodian-level data is data that is organized by custodian, such as email accounts, images of hard drives or hard drives themselves, or orphaned personal or home drives. It may contain data for several different clients or products. Although organizing data by custodian is not ideal, such data can be managed effectively if a comprehensive list of custodians subject to legal holds is maintained. Generally, effective remediation of custodian-level data is achieved by mapping the list of custodians subject to a legal hold with any data related to a custodian. An asset management database (which lists all assets or data "owned" by each custodian) and a holds management system (which lists all custodians subject to a legal hold) are helpful in effectively managing custodian-level data in a remediation project.

[A][3] Organizational-Level Data

Organizational-level data is data that is neither client-specific nor custodian-specific but is used by an organization for reporting purposes and managing its business. It includes financial records, personnel records, tax records, and training materials. Copies of organizational-level data are often made in connection with a legal hold; such copies are sufficient for the litigation or investigation, and therefore the original may not need to be retained in connection with a legal hold. There are usually specific record-retention policies associated with organizational-level data as well. Often organizational-level data is not the focus of remediation projects because the amount of data is limited, and the risks associated with the retention of the data are minimal.

[A][4] Media-Level Data (Including Backup Tapes)

Media-level data is a categorization of data by the type of media on which it is stored. Backup tapes are a difficult source of media-level data because they may contain different types of data—matter-specific, custodian-level, and organizational-level—or it may be unclear what type of data is located on them. Of course, other types of media, such as CDs, DVDs, USB drives, and hard drives, may also be maintained and stored without knowledge of their contents. But they differ from backup tapes insofar as their contents are easier to identify and index, and their data is likely to be viewed as readily accessible even though it is not on the active systems.

The remediation of unrecycled backup tapes requires extensive analysis, as discussed below in section 2:4.7, because the data on such tapes is not reasonably accessible and therefore not easily identified. Indeed, one process of remediation is to convert media-level data into more easily remediated categories, if appropriate. For example, backup tapes that contain email accounts or personal or home drives can be indexed and categorized as custodian-specific data for purposes of remediation.

[B] Noncentralized Data

Noncentralized data is data that is stored in an unstructured environment, often on a hard drive, personal/home drive or group/departmental shares on file server. Often, record management policies are not enforced effectively, and the risks associated with maintaining such data at the personnel level in an unstructured environment are high. An initial scoping for any remediation project should start with the determination of whether noncentralized data should be centralized so it can be properly remediated. At many organizations, IT departments or business units are creating large pockets of legacy data as data from personnel (usually departing personnel) is gathered and stored indefinitely (often at the request of the legal department). This data needs to be managed properly, and cross-referenced when any legal holds are initiated, as the risks of maintaining such data only increase over time and after an employee departs.

Potential ways to remediate this unstructured data held at the personnel level is discussed further in sections 2:4.8 and 2:4.9.

§ 2:4.6 Legal Standard for Knowledge About Legacy Data

Organizations are frequently confronted with legacy data sources in which data is not easily identifiable, such as unidentified backup tapes, unplugged and obsolete servers, and pallets full of other old equipment stored in warehouses. These sources may contain data

relevant to a pending investigation or litigation, but the costs and burdens of investigating the contents of the media are daunting. Balancing these costs and burdens with the risks of failing to disclose or produce potentially relevant data sources is a major challenge, particularly where there are inherent limitations in determining the contents of such media under normal circumstances because memories have faded, persons with relevant knowledge have departed, and scant records were kept.

Increasingly, courts are paying close attention to what steps are undertaken in searching for and producing information in discovery. Many courts cite Rule 26(g)(1) of the Federal Rules of Civil Procedure and relevant case law, which impose an "affirmative" duty on attorneys to determine whether there are potentially responsive documents in the possession, custody, or control of an organization subject to a discovery request. Rule 26(g)(1) requires a "reasonable inquiry" to determine whether discovery responses are sufficient and proper:

> [E]very discovery request, response, or objection must be signed by at least one attorney . . . . By signing, an attorney . . . certifies that to the best of [his or her] knowledge, information, and belief formed after *a reasonable inquiry*:
>
> . . .
>
> (B) with respect to a discovery request, response, or objection, it is:
>
> (i) consistent with these rules and warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law, or for establishing new law;
>
> (ii) not interposed for an improper purpose, such as to harass, cause unnecessary delay, or needlessly increase the cost of litigation; and
>
> (iii) not unreasonable or unduly burdensome or expensive, considering the needs of the case, prior discovery in the case, the amount in controversy, and the importance of the issues at stake in the action.[59]

In this context, "what is reasonable is a matter for the court to decide on the totality of the circumstances."[60] Presumably regulators would expect outside and in-house counsel to also conduct a "reasonable inquiry" for potentially responsive documents as part of their investigations or requests.

---

59. FED. R. CIV. P. 26(g)(1) (emphasis added).
60. FED. R. CIV. P. 26 advisory committee notes on 1983 amendment.

Courts have provided some guidance on what constitutes a "reasonable inquiry" under Rule 26(g), often defining the standard as objective reasonability under the circumstances.[61] A reasonable inquiry entails, at a minimum, implementing basic investigative procedures to discover potentially relevant documents, such as interviewing potentially knowledgeable personnel, reviewing documentation, and obtaining an understanding of an organization's procedures and processes for storing documents or ESI.[62]

However, absent special circumstances, the reasonable-inquiry standard likely would not impose a duty to search ESI on each piece of media, such as backup tapes, for relevant documents, in part because the reasonableness standard implies that there are cost considerations when determining what steps to take in an inquiry. In *Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc.*,[63] for example, the court denied a request for Rule 26(g) sanctions for failure to search backup tapes for relevant documents and noted that a "reasonable investigation to identify . . . relevant materials in the course of responding to . . . discovery requests . . . would not automatically include information maintained on computer back-up tapes."

---

61. *See, e.g.*, Phinney v. Paulshock, 181 F.R.D. 185, 203 (D.N.H. 1998) (duty under Rule 26(g) to make a reasonable inquiry "is satisfied if the investigation undertaken by the attorney and the conclusions drawn therefrom are reasonable under the circumstances").

62. *See* Qualcomm Inc. v. Broadcom Corp., No. 05 cv 1958-B, 2008 WL 66932, at *13 (S.D. Cal. Jan. 7, 2008), *vacated on other grounds*, 2008 WL 638108 (S.D. Cal. Mar. 5, 2008) (reasonable inquiry includes searching using "fundamental terms" on computers belonging to "knowledgeable people"); Metro. Opera Ass'n, Inc. v. Local 100 Hotel Emps. & Rest. Emps. Int'l Union, 212 F.R.D. 178, 221–24 (S.D.N.Y. 2003) (holding that counsel failed to comply with Rule 26(g) by, inter alia, failing to inquire about client's document storage procedures and capabilities, failing to implement systematic procedure for document production or retention, and failing to ask important witnesses for documents); Nat'l Ass'n of Radiation Survivors v. Turnage, 115 F.R.D. 543, 554–56 (N.D. Cal. 1987) ("[A] reasonable inquiry into the factual basis of [a party's] discovery responses . . . require[s], at a minimum, a reasonable procedure to distribute discovery requests to all employees and agents of the [party] potentially possessing responsive information, and to account for the collection and subsequent production of the information to [the opposing party].").

63. Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc., 244 F.R.D. 614, 628 (D. Colo. 2007); Young v. Pleasant Valley Sch. Dist., No. 3:07 cv 854, 2008 WL 2857912, at *3 (M.D. Pa. July 21, 2008) (rejecting plaintiff's request for production of emails located on backup tapes due to burden and expense).

A special circumstance likely would be where an organization has reason to believe that there is relevant ESI on the media that is not duplicative of ESI or documents from more accessible sources, such as an organization's active systems. However, even in this circumstance, it is likely that preservation and disclosure would be all that is required, and the legal standard as to whether production from a data source that is not reasonably accessible, in which a number of factors are considered, would be applied.

Thus, a "reasonable inquiry" by an organization facing the discovery of a collection of backup tapes (the most common situation today) likely would entail undertaking cost-effective steps to determine whether the backup tapes may contain potentially responsive ESI that is not duplicative of ESI on the organization's active systems. Such steps would include

- collecting and reviewing any documentation about the backup tapes;
- inspecting the tapes to see if there was any exterior indication which might provide information about their origin or what type of ESI they contain;
- interviewing the custodian of the tapes who could shed light on what ESI may be stored on them; and
- using any relevant documents to refresh the recollection of the custodian of the backup tapes.

A reasonable inquiry would not entail expending significant resources to actually search the ESI on the backup tapes for potentially relevant ESI. If, following a reasonable inquiry, the organization has reason to believe that potentially relevant ESI resides on the backup tapes and is not duplicative of ESI on the active systems, there may be a duty to disclose and possibly produce such ESI.

§ 2:4.7 *Remediation of Backup Tapes*

[A] Objectives

An organization may wish to undertake a comprehensive process to remediate unrecycled backup tapes, given that indefinite retention of backup tapes not subject to a litigation hold is neither a good business practice nor required by law.[64] The objective would be to

---

64. *See, e.g.*, Linnen v. A.H. Robins Co., No. 97-2307, 1999 WL 462015, at *1 (Mass. Super. Ct. June 15, 1999) ("The recycling of back-up tapes is, under normal circumstances, a widely accepted business practice as, in the absence of a disaster which necessitates the use of the tapes, there is

authorize backup tapes for recycling only after having conducted a reasonable, good faith effort to ensure that the organization has complied with its preservation obligations.[65]

Until the unrecycled backup tapes can be analyzed and unnecessary tapes recycled, the large number of tapes represents a substantial exposure to virtually unquantifiable litigation costs. Further, it is better to address the issue of backup tapes before it becomes an issue in litigation.[66] Finally there is no prohibition against changing approaches to document retention, even during litigation, so long as an organization takes a reasoned, deliberate approach to any deviations from established policy.[67]

A decision to recycle an organization's accumulated backup tapes must be made with cognizance of any obligations the organization may have to preserve documents in connection with actual or anticipated litigation or regulatory actions. The primary goal of the remediation process can be described as "inclusion and exclusion." As information about the tapes is gathered and analyzed, an organization will be able to make judgments about whether a tape or tape set should be included among the tapes to be preserved, or excluded from that group and recycled.

---

no need to keep them for an indefinite period of time."); Concord Boat Corp. v. Brunswick Corp., No. LR-C-95-781, 1997 WL 33352759, at *4 (E.D. Ark. Aug. 29, 1997) (reasoning that "to hold that a corporation is under a duty to preserve all email potentially relevant to any future litigation would be tantamount to holding that the corporation must preserve all email . . . such a proposition is not justified").

65. *See, e.g.*, Zubulake v. UBS Warburg LLC, 229 F.R.D. 422, 432 (S.D.N.Y. 2004) (*Zubulake V*) (recognizing that "reasonable steps" must be taken to identify documents subject to preservation obligations).

66. *See generally Linnen*, 1999 WL 462015, at *11 (imposing sanctions for failure to preserve backup tapes during litigation); Kleiner v. Burns, No. 00-2160-JWL, 2000 WL 1909470, at *4 (D. Kan. Dec. 22, 2000) (requiring party to disclose sources of electronic information, including backup tapes, under FED. R. CIV. P. 26(a)(1)).

67. *See* Drnek v. Variable Annuity Life Ins., No. CIV 01-242-TUC-WDB, 2004 WL 1098919, at *3 (D. Ariz. May 4, 2004), *aff'd*, 261 F. App'x 50 (9th Cir. 2007) (holding that absent any showing of destruction of relevant documents, implementation of a new document retention policy during litigation is not a basis for sanctions); *accord* Arthur Andersen LLP v. United States, 544 U.S. 696, 704 (2005) ("'Document retention policies,' which are created in part to keep certain information from getting into the hands of others, including the Government, are common in business. It is, of course, not wrongful for a manager to instruct his employees to comply with a valid document retention policy under ordinary circumstances." (citation omitted)).

To maximize efficiency and minimize cost, the secondary goal of the process is to allow inclusion and exclusion decisions to be made without the need to restore and review data from large numbers of backup tapes. Restoration and file-by-file review of the data on individual backup tapes is the most time-consuming and expensive part of any process of reviewing backup tapes. Thus, the process focuses on thorough information-gathering early on, in order to make inclusion and exclusion decisions about entire tapes and tape sets if possible, while minimizing the number of tapes that must be restored.

[B] Steps

The process generally would entail six major steps:

(1) Gather and assess information about the backup tapes and existing litigation and regulatory holds potentially applicable to these tapes.

(2) Conduct a "sweep" to ensure that reasonable steps have been taken to ensure that all unrecycled backup tapes have been properly located and identified.

(3) Develop a taxonomy of the tapes and holds.

(4) Follow up with business units to determine the possible business need for any information resident on the backup tapes.

(5) Exclude and include backup tapes for retention at the tape level or higher.

(6) As necessary, assess additional inclusion or exclusion models (for example, sampling tapes to eliminate additional data).

Each of these steps is outlined in general terms below. Completion of all of these steps requires the active involvement of a technological consultant.

[B][1] Gather Information

A party's efforts to comply with document holds must be tailored to that party's needs and capabilities.[68] Thus, the essential first step is for the organization to educate itself about the circumstances that it faces with respect to its backup tapes.

A detailed census of unrecycled backup tapes, and of the universe of holds that may apply to the tapes, will allow the organization to

---

68. *See, e.g.*, *Zubulake I*, *supra* note 34, at 323 (ruling that "the total cost of production compared to the resources available to each party" is one of the factors considered in cost-shifting analysis).

identify the techniques that will more accurately match data on backup tapes to potentially applicable holds. Given the potentially large number of backup tapes at issue, identifying appropriate methods of review is essential to developing a process that will minimize duplicated effort and expense. Moreover, courts have emphasized that counsel must have an understanding of a client's documents and document retention policies in order to effectively assist the client in complying with its preservation obligations.[69]

The information-gathering step can be broken down into two topics—the backup tapes and the hold systems.

[B][1][a] Tapes and Systems

Information related to the backup tapes, and the systems on which they were created, must be gathered in extensive detail. This will primarily entail interviews with, as well as written questionnaires and requests for information from, the organization's IT personnel responsible for the creation and maintenance of backup tapes. The objective is to develop a complete picture of the sources and organization of the data on the backup tapes, including the following:

- Information related to the software and hardware used to create the tapes, and on the tape specifications themselves;
- Information related to the backup process, including the type, timing, rotation, and retention of backups;
- Information related to any post-backup tape management system that may exist;
- Tape-set-specific information, including tape-set sizes and numbers;
- Sources of backup tapes other than from standard, periodic backups, including, for example, special-purpose backups for such things as data test sets, system migrations, audits, or special events like a merger; and
- Tape-specific information, including the types and numbers of tapes and the existence of any captured metadata about the tapes and/or backup sets.

---

69. *See, e.g.*, *Zubulake V*, 229 F.R.D. at 432. This does not, however, mean that every employee requires "hands-on supervision from an attorney." *Pension Comm. of the Univ. of Montreal Pension Plan, supra* note 31, at 473. The adequacy of each search must be evaluated on a case-by-case basis. *Id*.

[B][1][b] Holds

Information should also be gathered on the system for managing holds. It is important before commencing a remediation process that the organization confirm that the hold system is complete in that it covers "any relevant evidence over which [the organization] has control and reasonably knew or could reasonably foresee was material to a potential legal action."[70] Gathering information on the hold system will primarily entail interviews with and the collection of documentation from individuals knowledgeable in the use of the holds. For those holds which are prioritized as having potential applicability to the backup tapes, it will be necessary to discuss with counsel involved in those matters the types of information that have been produced and are potentially relevant. Important questions to answer at this stage include the following:

- What use can be made of any index and search capabilities of the hold system?
- What use can be made of any "type of claim" view in the hold system?
- How many holds are indicated in any reports as currently active?

[B][2] Conduct a Backup Tape Sweep

The second step involves conducting a physical sweep of the organization's facilities (including vendor facilities) where backup tapes might reasonably be found. As noted above, when an organization has a large volume of unrecycled backup tapes which it has already identified, it is likely that there are additional backup tapes within the organization that may need to be remediated. Focusing attention on only the known inventory without conducting additional searches for backup tapes may be deemed insufficient should an organization's efforts to ensure that it has properly preserved or produced relevant data ever be questioned.[71]

It must be emphasized that for any organization of significant size, it is unlikely that any backup tape sweep, no matter how comprehensive, will result in a collection of all backup tapes that are not in rotation. Backup tapes are typically stored in a variety of locations, many of them ad hoc and contrary to organization policy. Tapes may

---

70. China Ocean Shipping (Grp.) Co. v. Simone Metals Inc., No. 97-C 2694, 1999 WL 966443, at *3 (N.D. Ill. Sept. 30, 1999) (collecting cases).
71. *See* Coleman (Parent) Holdings, Inc. v. Morgan Stanley, Inc., No. CA 03-5045 AI, 2005 WL 674885, at *5–7 (Fla. Cir. Ct. Mar. 23, 2005) (entering partial default judgment against Morgan Stanley as sanction for its failure to do good faith search for backup tapes).

be found in employees' desks, in closets, and in off-site storage facilities. Accordingly, a realistic backup tape sweep policy will not purport to locate every backup tape in existence within the organization. Rather, it will consist of a set of reasonable steps designed to locate as many backup tapes as reasonably possible. The goal is a sweep that is, in light of electronic discovery industry standards, an objectively reasonable attempt to locate backup tapes.

[B][3] Create a Taxonomy of Backup Tapes and Holds

The third step involves analyzing the information gathered in the first two steps. The information is used to create a backup tape taxonomy that will allow the organization to identify which tapes, and how many tapes, belong to each tape set; the dates of each tape set; and, for each tape set, any available information on whether particular tapes correspond to particular sources of data or business units.

Likewise, the information on the hold system is used to create a detailed assessment of the scope and nature of the holds in the system. This information should allow the organization to identify the scope and nature of the holds currently in effect that are potentially applicable to data on the backup tapes. The critical analytical work at this step requires translating the information that describes the scope of the holds into rules that determine whether a particular backup tape or tape set is or is not subject to a hold.

Ideally, common fields of metadata will exist for both the taxonomy of backup tapes and the taxonomy of holds. For example, information on the creation date of a tape set can be matched against the date ranges for a hold to see whether the tape set could contain data potentially subject to the hold. This will permit the organization to more easily exclude or include tapes or tapes sets. By utilizing tape-set metadata, the organization can reliably identify which categories of backup tapes require further review and which do not. This process will reduce the cost associated with searching for data in the backup tapes.[72]

[B][4] Gather Information on Tape Use and Policies

Once the general nature and structure of the data on the backup tapes is understood, some follow-up information gathering will likely be required. It may be the case that certain business units have intentionally retained backup tapes for business purposes. Some interviews with business owners of backup tapes should reveal whether

---

72. *See* McNally Tunneling Corp. v. City of Evanston, Ill., No. 00 C 6979, 2001 WL 1568879, at *2 (N.D. Ill. Dec. 10, 2001) (refusing to require a party to "search through all of the documents based on the off-chance that certain [relevant documents] . . . were misfiled").

those tapes have been used for purposes other than disaster recovery. This process should help determine whether certain categories of tapes need to be retained because of business needs. It will also help an organization to identify those business groups that may need to be redirected towards more appropriate forms of long-term data retention than backup tape retention.

[B][5] Exclusion and Inclusion of Tapes or Tape Sets

Next, the organization applies the information gathered and organized in the previous steps to make decisions to exclude and include tapes. Where possible, complete tape sets or categories of tapes will be excluded. Where this is not possible, inclusion and exclusion decisions can be made for smaller groups of tapes or for individual tapes. For example, if it is determined that a given set of tapes likely contains data that is duplicative of data from more accessible data sources (for example, the data was migrated to a new server during an upgrade, and the tapes are a copy of what was migrated to the server), that set of tapes is primed for remediation.

This process must be directed and well documented by counsel,[73] possibly using statistical analysis to support the degree of confidence achieved.[74] When a decision is made to discard a tape, information about the tape and the reasons for disposition should be documented, so that the process of exclusion and inclusion produces an audit trail. The process must be executed in a manner that would permit a court or regulator to conclude that the holds were applied consistently and in good faith.[75] Retention of an expert witness to validate and opine on the appropriateness of the process employed would be valuable for this purpose.

[B][6] Additional Inclusion and Exclusion Techniques

By this time this step can occur, many backup tapes may have been excluded, though there may still be tapes for which a clear judgment of exclusion or inclusion could not be made. For these tapes, different techniques may be useful to reduce their numbers without resorting to restoring and reviewing large numbers of tapes at the file level.

Sampling of backup tapes is one such technique. It can be used to determine whether large numbers of backup tapes contain mostly redundant information, which would justify the recycling of tapes

---

73. *See, e.g.*, Danis v. USN Commc'ns, Inc., No. 98 C 7482, 2000 WL 1694325 (N.D. Ill. Oct. 23, 2000).
74. *See generally Zubulake I*, *supra* note 34, at 324 (endorsing the use of sampling to investigate contents of backup tapes); McKee v. Ashcroft, 202 F.R.D. 31 (D.D.C. 2001) (same).
75. *Lewy*, *supra* note 39, at 1112.

whose contents are largely duplicative of other tapes. For example, suppose full backups of the servers are made once a week and incremental backups of the servers are made each day. Since the full backup includes most of the data contained on the incremental daily backups, it should be possible to make reasonable inclusion and exclusion decisions without having to restore and search each day's incremental backup. Based upon an organization's risk tolerance (and in appropriate circumstances, after achieving authorization from a court or regulator), a similar analysis could be completed for "monthly" full backups, whereby only the last full backup of each month is retained for purposes of a legal hold.

Courts have endorsed sampling as a way to increase the effectiveness of searches of large amounts of data while reducing cost.[76] Sampling is appropriate because the rules governing discovery do not require parties to expend huge sums to search for a few potentially relevant documents that have not yet been found.[77] Consequently, redundant information need not be preserved, because a party has no obligation to search the same data twice.[78]

Whether sampling may be useful, and what type of sampling would be most effective and defensible, can only be determined upon reaching the final stage of the backup tape remediation process described above. Which techniques may be useful depends greatly on the information gathered about the backup tapes and tapes sets, and lessons learned during the inclusion-and-exclusion process.

[C] Results of the Inclusion-and-Exclusion Process

By the end of the inclusion-and-exclusion process, the number of accumulated backup tapes to be retained should be greatly reduced. For the tapes that remain, an organization will be in a position to

---

76. *See* Farmers Ins. Co. v. Peterson, 81 P.3d 659, 661–62 (Okla. 2003) (explicitly endorsing statistical sampling in the course of discovery of large amounts of paper and electronic data).

77. *See* Cognex Corp. v. Electro Sci. Indus., Inc., No. Civ. A. 01 CV 10287 RCL, 2002 WL 32309413, at *5 (D. Mass. July 2, 2002) (refusing to order a search of backup tapes, even at requester's expense, when the responding party "has already conducted an extensive search for relevant documents. At some point the adversary system needs to say 'enough is enough' and recognize that the costs of seeking every relevant piece of discovery is not reasonable.").

78. *See, e.g.*, Hussey v. Chase Manhattan Bank, No. Civ. A. 02-7099, 2004 WL 220845, at *2–3 (E.D. Pa. Jan. 12, 2004) (holding that it was unnecessary to search electronic email archive when identical paper archive has already been searched).

determine the efficacy and desirability of approaches for ongoing tape retention or review. By undertaking the inclusion-and-exclusion process after a single, comprehensive sweep, and by minimizing the use of restoration and file-by-file review of backup tape contents, an organization will avoid the prohibitive expense of conducting multiple reviews of all of the backup tapes in future litigation. It will instead have to conduct, at most, only limited restoration of a smaller number of tapes in individual litigations—a smaller, quantifiable expense that can be controlled through the use of the taxonomy of backup tapes, further sampling, and other methods at an organization's disposal.

[D] Resumption of Recycling of Daily Backup Tapes

An organization should undertake a comprehensive process to confirm that it is in compliance with all current and anticipated holds, and based on this process, it can resume recycling of its daily backup tapes and consider resuming the recycling of other backup tapes. The legal principles supporting the resumption of recycling of an organization's backup tapes are similar to those supporting the remediation of an organization's legacy backup tapes, described above, and much of the work done during the remediation process, especially the taxonomy of holds, will be applicable here also. The resumption of recycling of backup tapes should be accompanied by the development and implementation of comprehensive backup tape policies on a going-forward basis as well as a comprehensive legal memorandum setting forth the justification for the resumption of recycling.

§ 2:4.8 Remediation of Accumulated Images of Hard Drives and Other Custodian-Level Data

An organization should undertake a comprehensive process to remediate its accumulated imaged hard drives and other custodian-level data sources, such as orphaned home or personal drives and email accounts of departed employees. As with unrecycled backup tapes, the accumulated custodian-level data sources represent a substantial exposure to litigation costs for an organization. An organization's objective with respect to accumulated custodian-level data sources should be to conduct a reasonable, good faith effort to ensure that it has complied with its preservation obligations before these data sources are authorized for disposal. This effort should include procedures designed to ascertain whether the data associated with a custodian must be preserved for any litigation or investigation. Much of the work product from the backup tape remediation process described above, including the gathering of information on legal and regulatory holds and the development of the taxonomy of holds, will be equally usable in the custodian-level data remediation process.

It bears emphasis that the custodian-level data source remediation process should include the development of collection procedures from custodians that, in appropriate cases, will provide the organization with an alternative to imaging the entire hard drive, or collecting the whole home or personal drive and email account of a business user. For example, it may sometimes be appropriate to limit collection to only relevant electronic information on a custodian's hard drives, personal or home drive, or email account (by using search terms or identified folders with relevant information), thus creating a matter-specific data source which is easier to manage and remediate. If an organization concludes that its collection methods should be broad, whereby hard drives are imaged and collected, and all files in home or personal drives and email accounts are copied for collection, the custodian-level data source remediation process should also include the development of policies and processes for disposal of the custodian-level data sources promptly after relevant information is collected from them.

§ 2:4.9 *Remediation of Legacy Data in Possession of Employees*[79]

An organization's remediation efforts should include some determination as to what to do with ESI in the possession of its personnel, much of which may be legacy data that should be subject to remediation (that is, data not needed for any present business purpose, apart from record retention policies, and not subject to an existing legal hold). Such ESI, including legacy data that is subject to an active, existing legal hold, may need to be considered in connection with new requests for information from civil litigants and government agencies and regulators. The problem, however, is that such data has often not been centralized, so that there is no single repository which can be searched and indexed when necessary. Thus, an organization may be forced to rely on personnel to correctly identify and preserve relevant ESI, as well as to take appropriate steps when a legal hold associated with ESI in their possession is lifted. Such reliance may be both risky and inefficient. This section discusses the challenges and approaches to remediating ESI currently in the possession of an organization's employees.

---

79. This section is heavily indebted, both in terms of structure and information, to Ryan P. Farley and Anthony J. Diana, *Remediation of Electronic Data in the Possession of Employees*, THE LEGAL INTELLIGENCER, Feb. 4, 2008, at ED7–ED8.

[A] Challenges

There are a number of significant challenges that are specific to the remediation of ESI in the possession of personnel, as opposed to the remediation of ESI that is located in centralized locations or in collections on servers. These challenges include:

- **Communication with personnel:** Careful consideration should be paid to the timing and mode of communication with personnel, so that the risk of misunderstanding is minimized (for example, so that personnel subject to more than one hold do not misinterpret instructions authorizing the lifting of one hold as authority to lift all holds).
- **Difficulty in auditing compliance by personnel:** The responsibility for locating and remediating ESI that is no longer associated with a hold falls largely on the personnel, so extensive follow-up, or even compliance audits might be required to ensure that personnel comply with notifications that holds have been lifted.
- **Lack of uniformity in personnel data preservation:** The almost inevitable differences among personnel in their methods of preserving data (that is, the lack of uniformity and organizational clarity with respect to how and where they stored data) will likely make the remediation process more time- and energy-intensive, and will, in turn, decrease the probability of successful remediation by personnel.

[B] Approaches

There are four approaches to remediating ESI in the possession of personnel: (1) centralization of all data subject to a hold issued by legal counsel; (2) legacy data remediation performed by the personnel themselves; (3) comprehensive personnel legacy data sweeps by a designated team or teams of professionals; and (4) exclusion of personnel legacy data from any organization-wide remediation project.[80]

As discussed below, each approach offers distinct advantages and disadvantages. It may thus be appropriate to pursue a blended approach, for example, centralizing legacy data for remediation and ongoing management in more sensitive areas, such as regulatory matters and litigations, while relying upon personnel to remediate legacy data associated with less sensitive matters, such as nonparty subpoenas.

---

80. There is technology now available to help remediate unstructured data in the possession of personnel, but it is a costly alternative.

[B][1] Centralization

The first option for remediating ESI in the possession of personnel is to collect all ESI (including both legacy data and active holds data) and provide that its continuing preservation and/or remediation will be handled by the organization's designee. The benefits of this approach are that it (1) reduces the number of legacy data sources to be considered in connection with new requests, (2) takes the responsibility of preserving and searching legacy data out of the hands of personnel, and (3) avoids the potential problems of tasking personnel with the job of remediating legacy data in their possession (as discussed below).

There are, however, some problems associated with this approach if it is applied to all personnel and all existing holds. First, notifying personnel about existing holds and collecting all relevant ESI is likely to be time-consuming and very costly for the organization.[81] Second, organizing the data for collection is likely to be time-consuming for the personnel as well, which could impact productivity at the organization. Finally, there is also the risk of personnel making mistakes while collecting and organizing ESI (and potentially deleting or discarding ESI they believe is no longer subject to a hold).

[B][2] Data Remediation by Personnel

The second option for remediating ESI in the possession of personnel is to rely upon the individuals themselves to remediate the legacy data (and continue to preserve the data subject to an active hold). Under this approach, upon being informed of a hold being lifted, the personnel would determine what ESI in their possession should be returned to normal handling under the applicable records retention policies.

The appeal of this approach is that it disperses the work of remediation among the organization's personnel. The potential problems include the risk of mistakes in remediating data, and the risk of miscommunication when notifying personnel of the hold status of ESI in their possession.

---

81. This is true regardless of whether an organization opts for manual collection (requiring each personnel to identify the data associated with a particular hold applicable to that personnel, and to transmit the data to a specified custodian/location on a CD, DVD, or some other medium, as well as to physically transfer some of it) or automated collection (utilizing remote collection technology to collect data from an identified folder on the personnel's computer desktop, and physically shipping the hard copy documents that cannot quickly or efficiently be PDF'd or TIFF'd).

[B][3] Office-by-Office, Person-by-Person Remediation

The third approach for remediating ESI in the possession of personnel is to have teams go through the individual offices of personnel and work with them in identifying and addressing ESI associated with holds that have been lifted. This is likely to be a substantial undertaking, which would involve logistical complexity, and expenditure of significant time and resources. Nevertheless, this is the most comprehensive way to achieve results, and from a legal standpoint, one that may also be straightforward to explain and defend.

One way to reduce the amount of time and resources necessary for this approach is to limit the number of personnel involved, by targeting only those employees most likely to have significant amounts of ESI, or confining the remediation effort to the largest departments or offices, or those departments or business units with significant legal or regulatory risks associated with their ESI.

[B][4] Exclusion of Personnel Data from Any Remediation Project

The fourth option is to forego the remediation of data in the possession of personnel altogether, and to instead remediate only centralized ESI. This option may be appropriate for an organization that already has a significant volume of centralized ESI subject to historic holds. It is appealing because it saves personnel time, and avoids the dangers of their mistakenly destroying ESI in their possession.

The downside of excluding personnel data from a remediation project is that nonremediated ESI continues to grow and remains a potentially responsive source of data that must be considered in response to each new request for information. Further, this approach results in the preservation obligations remaining with the personnel.

§ 2:5 Trends

Over the past several years, the burdens imposed by electronic discovery have changed, as have the expectations of companies' technological capabilities. Data that may once have been inaccessible due to undue burden and cost may now be accessible if stored properly. As a result, courts and regulators increasingly expect organizations to always be prepared for litigations and investigations.

§ 2:5.1 Managing Risks of Deletion of ESI

There are several things that organizations can do to help manage the risks associated with potential deletion of ESI relevant to a litigation or investigation. They can take steps to make data more accessible and reduce the opportunities for information to be lost during

routine operations. This can be done, for example, through the use of email archive systems that keep data active for long periods of time. However, the costs of such an archiving system can be prohibitive if not managed correctly (such as by having a policy and process for purging after an appropriate retention period) and if there is not a robust and sophisticated method for managing the increased amount of accessible data in litigations and investigations (such as by the use of advanced technology, search terms, and conceptual searching techniques to minimize the cost of processing data and review for responsiveness and privilege).

The highest-profile risks coincide with policies involving deliberate deletion or overwriting of information. For example, in the case of *In re Krause*,[82] a debtor who failed to disable a wiping software program (Ghost Surf) after a duty to preserve arose argued that the resulting losses were merely the result of a routine and good faith operation of electronic systems exempt from sanctions under amended Rule 37. The court concluded, however, that it was "improbable" that the overwriting was routine, given the fact that the hard drives were "far from being at full capacity."[83]

The classic example of misunderstanding, however, is found in the dueling opinions rendered in *Rambus v. Infineon Technologies*[84] and *Hynix Semiconductor v. Rambus*.[85] Both cases reviewed the same evidence involving implementation of a document retention policy, which featured shortened recycling of backup media and institution of "shred days," at the same time a litigation strategy was implemented to enforce patent rights. The two courts reached diametrically opposed conclusions on the motivation for the records retention program. For the *Infineon* court, it was clearly designed to eliminate potentially damaging documents that a future adversary might discover; for the *Hynix* court, however, the motivation was to reduce unnecessary nonmaterial information, which did not involve spoliation.[86]

Suspicions about motivation can also arise when parties fail to negate the automatic deletion of email once a preservation duty is

---

82. *In re* Krause, 367 B.R. 740 (Bankr. D. Kan. 2007).
83. *Id*. at 768.
84. Rambus v. Infineon Techs., 222 F.R.D. 280, 298–99 (E.D. Va. 2004).
85. Hynix Semiconductor v. Rambus, 591 F. Supp. 2d 1038 (N.D. Cal. 2006), *aff'd in part*, *vacated in part*, *and remanded by* 645 F.3d 1336 (Fed. Cir. 2011).
86. In a third case, Samsung Elecs. Co. v. Rambus, 439 F. Supp. 2d 524, 566 (E.D. Va. 2006), *vacated in part*, *and remanded by* 523 F.3d 1374 (Fed. Cir. 2008), the same Virginia district court judge criticized the decision in *Hynix* as "not persuasive" and argued that it involved accepting testimony which was not "credible."

triggered.[87] In *Mosaid Technologies, Inc. v. Samsung Electronics Co.*,[88] an "automatic computer email policy allowed emails to be deleted, or at least to become inaccessible, on a rolling basis." In *Wingnut Films, Ltd. v. Katja Motion Pictures Corp.*,[89] "every employee's email inbox is purged every 30 days, and . . . the backup tapes are wiped clean on a weekly basis."[90] In *Connor v. Sun Trust Bank*,[91] the district court sanctioned the defendant employer for failure to produce a supervisor's email that was later "destroyed by operation of [the] automatic deletion of emails that are more than thirty days old and not archived." The court was convinced that "the only way" the email could not have been found by the supervisor prior to the automatic deletion would have been if the supervisor had deliberately deleted it in "bad faith."[92]

Moreover, organizations can manage the risk of potential deletion of relevant ESI by implementing programs that preserve and collect data from external sources, such as USB drives, handheld devices, or iPods, that are often susceptible to inadvertent deletion of data. A particular area of risk is BlackBerry devices or similar devices which are not set for retention policies similar to those of the email server.

---

87. The earliest reference found to such an approach is in Samuels v. Mitchell, No. C 91-20377 RPA, 1995 WL 936327 (N.D. Cal. Jan. 18, 1995), where the court refused to impose sanctions for the use of a "janitor" program which would notify email users that messages over ninety days old would be moved to a wastebasket unless the user acted to preserve them. The court held that the "system was used properly and in no way was used to willfully destroy evidence." *Id*. at *2.

88. Mosaid Techs., Inc. v. Samsung Elecs. Co., 348 F. Supp. 2d 332, 333 (D.N.J. 2004) (affirming Magistrate Judge Hedges) (upholding sanctions against Samsung for willfully blinding itself to the fact that negligent destruction of email can lead to loss of relevant evidence).

89. *Wingnut Films*, *supra* note 50, at *14–17 (granting direct access by jointly selected outside vendor, at defendant's cost, to defendant's servers and the hard drives of specified employees' work stations and laptops for purpose of producing log of contents based on keyword searches for responsive documents and emails); citing Tulip Computs. Int'l B.V. v. Dell Comput. Corp., No. CIV. A 00.981-RRM, 2002 WL 818061 (D. Del. Apr. 30, 2002).

90. *Id*. at *14.

91. Connor v. Sun Tr. Bank, 546 F. Supp. 2d 1360, 1376 (N.D. Ga. 2008) (announcing decision to give jury instruction based on inference).

92. The email was subsequently recovered by other means. *Id*. at 1377. For a discussion of the requirements of production of email metadata, see O'Neill v. City of Shoreline, 170 Wash. 2d 138 (Wash. 2010) (Supreme Court of Washington, in a case of first impression, held that metadata is subject to disclosure pursuant to Washington's Public Records Act).

Where the auto-deletion function for the email server is set to leave emails in place only for a short length of time, the handheld devices may end up being the primary source of email. Organizations should be prepared to demonstrate that whatever policies and procedures are implemented for such devices, the approach taken was reasonable after balancing the risks of potentially relevant and nonduplicative ESI being stored on such devices, and the risks that such ESI may be deleted either automatically or by the end user.

Courts are often intolerant of a party's failure to implement a litigation hold, and thus steps should be taken to implement policies and procedures that can help shield the organization from liability based on the actions of its employees. Rule 37(e) of the Federal Rules of Civil Procedure requires parties to "take reasonable steps to preserve" ESI that is or would be subject to a litigation hold.[93] The Rule differentiates between instances where a party negligently fails to preserve ESI from situations where a party "acted with the intent to deprive another party of the information's use in the litigation," reserving the more severe penalties available under the Rule—an adverse inference or case dismissal—for the latter.[94] Having an organizational policy addressing the routine operational retention, and removal, of electronic information can help to frame the discussion of conduct of an employee who negligently deletes electronic information subject to a litigation hold. In *Escobar v. City of Houston*,[95] for example, the court refused to sanction the failure to interrupt the routine overwriting of audio tapes in the absence of any showing of the loss of relevant information or that the producing party acted in bad faith. In *Lockheed Martin Corp. v. L-3 Communications Corp.*,[96] the court refused to

93. FED. R. CIV. P. 37(e).

94. FED. R. CIV. P. 37(e) provides that "if electronically stored information that should have been preserved" was "lost because a party failed to take reasonable steps to preserve it" then "upon a finding that the party acted with the intent to deprive another party of the information" a court may "presume that the lost information was unfavorable to the party[,] instruct the jury that it may or must presume the information was unfavorable to the party; or [ ] dismiss the action or enter a default judgment." This provision was part of the 2015 amendment to Rule 37(e).

95. Escobar v. City of Houston, No. 04-1945, 2007 WL 2900581, at *18 (S.D. Tex. Sept. 29, 2007) (citing to the former Rule 37(f) and noting arguments of loss of relevant information and evidence of efforts to preserve relevant information).

96. Lockheed Martin Corp. v. L-3 Commc'ns Corp., No. 605CV-1580-ORL-31 KRS, 2007 WL 3171299, at *2 (M.D. Fla. Oct. 25, 2007) ("there is no evidence that the email he deleted falls within the category").

sanction the acts of an employee in "cleaning up" his email where he did not recall receiving a litigation hold order and there was no indication that the information had not been otherwise produced.[97]

However, there is a risk that a court will conflate the obligations of employees with those of their employers.[98] The *Zubulake* line of cases simply assumed without discussion that any acts or failures are attributable to the employer. A more nuanced approach was taken in *Hawaiian Airlines, Inc. v. Mesa Air Group*,[99] where the CFO deliberately scrubbed email from two laptops after being notified of the need to preserve. The actions were attributable to the party[100]—but it was also blamed for its failure to anticipate the issue and thus make a copy of the hard drives. It was not enough, the court said, to simply trust the employee to comply, given the risk that such high-level employees might do "wrongful and foolish things, like destroying evidence, under the pressure of litigation."[101]

To address these concerns, organizations should create, and constantly revise, written policies and procedures for the storage and maintenance of ESI. As described earlier in this chapter, the policies and procedures should:

- contemplate relevant regulatory schemes;
- be drafted in conjunction with both business and information technology employees;
- consider data retention and recycling;

---

97. After the testimony concerning deletion of emails done to "clean up," a forensic examination of the hard drive of the workstation computer was also undertaken. *Id*.

98. *See* Doe v. Norwalk Cmty. Coll., 248 F.R.D. 372, 378 (D. Conn. 2007) (refusing to consider Rule 37(e) because there was not "one consistent, 'routine' system in place" regarding email management); Okla. *ex rel*. Edmondson v. Tyson Foods, Inc., No. 05-CV-329-GKF-SAJ, 2007 WL 1498973, at *6 (N.D. Okla. May 17, 2007) ("The Court . . . advises the parties that they should be very cautious in relying upon any 'safe harbor' doctrine as describe in new Rule 37(f).").

99. Hawaiian Airlines, Inc. v. Mesa Air Grp., Nos. 03-00817, 06-90026, 2007 WL 3172642 (Bankr. D. Haw. Oct. 30, 2007).

100. *Id*. at *6–7 ("He acted in the course and scope of his employment, in an attempt to further Mesa's interests, using Mesa's computer equipment. . . . [and] had a motive to conceal documents that could have proven the falsity of his own testimony.").

101. *Id*. at *5 ("Mesa could have taken reasonably steps that would have prevented, or mitigated the consequences of, Mr. Murname's destruction of evidence. . . . Doing so [making "backups" of hard drives after suit was filed] would not have been costly, burdensome, or unduly disruptive of Mesa's business.").

- allow for the easy implementation of a litigation hold; and
- include a disaster recovery plan.

Organizations should retain an individual (or an outside expert) who understands the companies sources of ESI and who can, if necessary, testify about those sources of data.

§ 2:5.2 Requiring Investment in Technology

Will a party which suffers frequent requests for production of communications be required to invest in extended storage technology to facilitate preservation and production?

Currently, courts take the preservation schema of an entity pretty much as it exists at the time a dispute arises. The U.S. Supreme Court in *Oppenheimer Fund, Inc. v. Sanders*[102] stated that it "borders on the frivolous" to argue that a party should be penalized for not keeping its records "in the form most convenient to some potential future litigants identity and perceived needs could not have been anticipated." In *Malletier v. Dooney & Bourke, Inc.*,[103] the court refused to require a party to create a business process to preserve temporary communications posted in chat rooms.

However, some courts have suggested contrary views. In the early-1990s case of *PHE, Inc. v. Department of Justice*,[104] the court candidly ordered the producing party to "incur modest additional expenditures" to provide discovery from databases not programmed to produce the information required.[105] In the more recent case of *Zurich American Insurance v. Ace American Reinsurance Co.*,[106] a magistrate judge offered "little sympathy for [a party] utilizing an opaque data storage system, particularly when, by the nature of its business,

---

102. Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340, 363 (1978).
103. Malletier v. Dooney & Bourke, Inc., No. 04 CIV. 5316, 2006 WL 3851151, at *2 (S.D.N.Y. Dec. 22, 2006) (no duty exists to install a system to monitor and record communications in order to retain chat room comments).
104. PHE, Inc. v. Dep't of Justice, 139 F.R.D. 249, 257 (D.D.C. 1991).
105. *See* Thomas Y. Allman & Kevin F. Brady, *Does RAM Discovery Make Good Law?*, NAT'L L.J., Dec. 10, 2007 (noting that Nat'l Union Elec. v. Matsushita Elec. Indus. Co., 494 F. Supp. 1257 (E.D. Pa. 1980), held that "common sense" required production in machine-readable format despite the fact that the information did not exist in that precise form).
106. Zurich Am. Ins. v. Ace Am. Reinsurance Co., No. 05 CIV. 9170, 2006 WL 3771090 (S.D.N.Y. Dec. 22, 2006).

it can reasonably anticipate frequent litigation." The court in *W.E. Aubuchon Co. v. BeneFirst, LLC*[107] also criticized as "inexplicable" the programming of a database which made it difficult to access group claims, and the court denied any attempt to shift the costs of access.

To date, the suggestion that investments are part and parcel of the duty to preserve and produce is probably a bridge too far. In *Procter & Gamble Co. v. Haugen*,[108] the court of appeals reversed an order of s anctions because the preservation steps not taken would have required installation of a new server or the purchase of archival data from a third party. However, it is not hard to imagine that under some circumstances, this is a bridge that will be crossed.

§ 2:5.3 Internal Social Media Policies

Social media is increasingly becoming an important source of potentially relevant information, particularly in criminal, personal injury, employment, and family law cases. Social media is becoming an important tool in the business context as well, given that many companies have blog posts, Facebook pages, and Twitter accounts. Moreover, company employees are increasingly being allowed to use their personal devices to do their work. These developments are imposing obligations on businesses to preserve, collect, and produce social media which has become a useful source of evidence in a variety of cases, ranging from securities litigation to defamation, misappropriation of trade secrets, breach of confidentiality, breach of noncompete agreements, copyright and trademark violations, tortious interference, and regulatory violations. Organizations must stay attuned to developments, particularly as courts begin to create and apply laws to this area of instability. Since the social media landscape is far from settled, organizations must exercise significant caution to avoid liability, including overseeing business activities.[109]

"Social media" refers to Internet-based technologies and websites that allow individual or organizational users to publish content to a wider audience, including professional networks, prospective marketing contacts, and clients. Sites such as LinkedIn, Facebook, YouTube and Twitter provide opportunities and challenges for organizations. Yet, preventive measures can be taken to reduce the risks associated with social media, including steps by in-house and outside counsel.

---

107. W.E. Aubuchon Co. v. BeneFirst, LLC, 245 F.R.D. 38, 41 (D. Mass. 2007).
108. Procter & Gamble Co. v. Haugen, 427 F.3d 727 (10th Cir. 2005).
109. *See generally* THE SOCIAL MEDIA REVOLUTION: A LEGAL HANDBOOK (John Nadolenco ed., Mayer Brown) (2010).

An organization's general liability policy may not include social media use, leaving employers at risk for vicarious liability for employee acts within the scope of their employment. As a result, companies should have specific policies that address social media, with guidelines and procedures governing appropriate social media use, including use of networking sites, blogs, and other media platforms. Procedures may be global or tailored to individual media platforms.[110]

Other considerations when dealing with social media include whether it is used on behalf of the entire company, or, purposefully or not, through personal employee online communications. In the case of personal employee communications, disclaimers may be an option to indicate that employees may not be speaking on behalf of the company. Some organizations may even issue prohibitions on references to the company, unless done with corporate approval.[111]

Managing internal social media policies requires examination of various aspects of an organization, such as

- company websites or company-owned websites, with an eye toward potential legal concerns;
- issues concerning social media and legal ethics, including conflicts of interest, the duty of confidentiality to a client, lawyer advertising and solicitation, improper publicity, unauthorized practice of law, contact with other parties to a matter, the duty of candor, decorum and impartiality of the tribunal, misconduct, and responsibility for subordinates;
- social networking in employment decisions, social networking monitoring during employment, and what employers can do when employment ends;
- how jurisdictional aspects of litigation may be impacted.[112]

When drafting a social media policy, relevant considerations may include

- what overarching goals and reasons exist for engaging in social media;
- what social networks/media sites are authorized/restricted;
- how to protect confidential or proprietary information, such as trademarked information, and how to comply with copyright and fair-use laws;

---

110. *Id.*
111. *Id.*
112. *Id.*

- how to alert employees about PR and liability issues related to discussion of clients or business contacts in online forums;
- how to encourage professional standards of conduct, including avoiding inflammatory or other statements that may expose the organization to liability;
- specific information that should not be disclosed, such as financial or legal information;
- how to encourage reporting of violations of a social media policy;
- how to alert employees that online social media will be monitored and retained in order to comply with policies and regulations;
- how to alert employees that online actions may be modified or deleted, if necessary;
- how to examine the differences in usage of company property (equipment and networks) versus personal property;
- the follow-up steps for dealing with violations of the social media policy; and
- the parties tasked with monitoring the policy or potential violations.

In recent years, courts have increasingly faced questions regarding social media sites and the duties of production in litigation, including issues such as whether the information on social media is considered private, whether it is discoverable, and whether it is admissible as evidence.[113]

---

113. *See, e.g.*, Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965 (C.D. Cal. 2010) (upholding a subpoena, including Facebook "wall posts" and web comments accessible to the general public as discoverable); *In re* Facebook PPC Advert. Litig., No. C09-3043 JF (HRL), 2011 WL 1324516 (N.D. Cal. Apr. 6, 2011) (despite Facebook's resistance, granting plaintiffs' motion to compel Facebook's participation in the creation of an ESI Protocol; ordering Facebook re-produce ESI in native format); Reid v. Ingerman Smith, LLP, No. CV 2012-0307, 2012 WL 6720752 (E.D.N.Y. Dec. 27, 2012) (granting in part motion to compel production of plaintiff's Facebook page in sexual harassment case because it provided probative evidence of her mental and emotional state). For an in-depth discussion of email privacy, see United States v. Warshak, 631 F.3d 266 (6th Cir. 2010) (finding that an email subscriber enjoys a reasonable expectation of privacy in the contents of his emails that are stored with, or sent or received through, a commercial ISP and that the government may not compel a commercial ISP to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause).

Recent court rulings have underscored the duty to preserve social media once litigation is pending, and they have begun to impose sanctions when parties have failed to do so.[114]

114. *See, e.g.*, Gatto v. United Airlines, No. 10-CV-1090-ES-SCM, 2013 WL 1285285, at *5 (D.N.J. Mar. 25, 2013) (jury could draw adverse inference against plaintiff for failure to preserve evidence when he deactivated his Facebook account, resulting in permanent loss of account data); Christou v. Beatport LLC, No. 10-CV-02912-RBJ-KMT, 2013 WL 248058, at *14 (D. Colo. Jan. 23, 2013) (declining to allow adverse inference instruction, but allowing plaintiffs to introduce evidence at trial to show defendants failed to preserve text messages after key defendant's phone was lost).