IMPORTANT NOTICE:
This Publication Has Been Superseded

See the Most Current Publication at

https://thesedonaconference.org/publication/Commentary_on_Defensible_Disposition

wgs

The Sedona Conference

Principles and Commentary on Defensible Disposition

A Project of The Sedona Conference
Working Group on Electronic Document
Retention & Production (WG1)

August 2018
Public Comment Version
Deadline to submit comments extended to **October 24, 2018**.
Send to comments@sedonaconference.org.

The Sedona Conference
Principles and Commentary on Defensible Disposition

A Project of The Sedona Conference Working Group on
Electronic Document Retention and Production (WG1)

AUGUST 2018 PUBLIC COMMENT VERSION

Author: The Sedona Conference

Drafting Team

Lauren A. Allen
Ross Gotler
Logan J. Herlinger
Mark Kindy
Jesse Murray
Ken Prine
David C. Shonka

WG1
Drafting Team Leaders

Tara Emory
Becca Rausch

Editors-in-Chief &
Steering Committee Liaisons

Kevin F. Brady
Dean Kuckelman

Staff Editor: Susan McClain

We thank all of our Working Group Series Annual Sponsors; whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors, just click on the "Sponsors" navigation bar on the homepage of our website.

Preface

Welcome to the 2018 Public Comment Version of The Sedona Conference *Principles and Commentary on Defensible Disposition*, a project of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, and intellectual property rights. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

The idea for this *Commentary* arose from discussion in 2016 among the Steering Committee liaisons and team leaders in charge of updating the 2014 *Commentary on Information Governance* which was a topic for discussion at the Sedona Conference WG1 2016 Midyear Meeting. The leadership recognized that with the staggering amount of data that is produced daily, there was a need for guidance for organizations and counsel on the adequate and proper disposition of information that is no longer subject to a legal hold and has exceeded the applicable legal, regulatory, and business retention requirements. At the 2016 Annual Meeting, the subject of defensible disposition as a separate topic was first discussed where it received a very favorable reception. Then at the 2017 Midyear Meeting, there was a session dedicated exclusively to "Defensible Disposition of Information." As a result of that panel discussion and the dedicated work of the drafting team, a preliminary draft of this *Commentary* was presented for member comment at the 2018 Midyear Meeting. Based on member feedback, the drafting team has prepared this final draft to be released for public comment.

The Sedona Conference acknowledges the efforts of Drafting Team Leaders Tara Emory and Becca Rausch, who were invaluable to driving this project forward. We also thank drafting team members Lauren A. Allen, Ross Gotler, Logan J. Herlinger, Mark Kindy, Jesse Murray, Ken Prine, and David C. Shonka for their efforts and commitments in time and attention to this project. Finally, we thank Kevin Brady and Dean Kuckelman who served as both the Editors-in-Chief and WG1 Steering Committee Liaisons to the drafting team.

Please note that this version of The Sedona Conference *Principles and Commentary on Defensible Disposition* is open for public comment through October 10, 2018, and suggestions for improvement are very welcome. After the deadline for public comment has passed, the drafting team will review the public comments and determine what edits are appropriate for the final version. Please submit comments by email to comments@sedonaconference.org.

In addition, we encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG1 and several other Working Groups in the areas of international electronic information management, discovery, and disclosure; patent damages and patent litigation best practices; data security and privacy liability; trade secrets; and other "tipping point" issues in the law. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it

should be. Information on membership and a description of current Working Group activities is available at https://thesedonaconference.org/wgs.

Craig Weinlein
Executive Director
The Sedona Conference
August 2018

Table of Contents

I. INTRODUCTION

Principle 6 of The Sedona Conference *Commentary on Information Governance* provides the following guidance to organizations:

> The effective, timely, and consistent disposal of physical and electronic information that no longer needs to be retained should be a core component of any Information Governance program.[1]

The Comment to Principle 6 explains:

> It is a sound strategic objective of a corporate organization to dispose of information no longer required for compliance, legal hold purposes, or in the ordinary course of business. If there is no legal retention obligation, information should be disposed as soon as the cost and risk of retaining the information is outweighed by the likely business value of retaining the information. . . . Typically, the business value decreases and the cost and risk increase as information ages.[2]

Despite this advice, and similar advice from other sources, many organizations continue to struggle with making and executing effective disposition decisions. That struggle is often caused by many factors, including the incorrect belief that organizations will be forced to "defend" their disposition actions if they later become involved in litigation. Indeed, the phrase "defensible disposition" suggests that organizations have a duty to defend their information disposition actions. While it is true that organizations must make "reasonable and good faith efforts to retain information that is relevant to claims or defenses," that duty to preserve information is not triggered until there is a "reasonably anticipated or pending litigation"[3] or other legal demands for records. Another factor in the struggle toward effective disposition of information is the difficulty in appreciating how such disposition reduces costs and risks. Lastly, many organizations struggle with *how* to design and implement effective disposition as part of their overall Information Governance program.

These Principles and Commentary regarding disposition of information ("Commentary") attempt to address these three factors and provide guidance to organizations, and the professionals who counsel organizations, on developing and implementing an effective disposition program. This paper uses "information" to refer to both physical and electronic information.

---

1 The Sedona Conference, *Commentary on Information Governance*, 15 SEDONA CONF. J. 125, 146 (2014). "Information Governance" is "an organization's coordinated, interdisciplinary approach to satisfying information compliance requirements and managing information risks while optimizing information value." *Id.* at 126.

2 *Id.* at 147.

3 *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONF. J. 1, 51, Principle 5, 93 (2018).

II. PRINCIPLES

PRINCIPLE 1. Absent a legal retention or preservation obligation, organizations may dispose of their information.

Comment 1.a. An organization should, in the ordinary course of business, properly dispose of information that it does not need.

Organizations may avoid retaining information that is not subject to retention or preservation obligations.[4] Regular disposition of obsolete information is simply a best information management practice, related to good housekeeping and Information Governance, which was acknowledged by the United States Supreme Court in *Arthur Andersen LLP v. United States*:

> '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.[5]

In *Andersen,* the Court reversed and remanded a criminal conviction under a federal obstruction statute, noting that "[a] 'knowingly corrupt persuader' cannot be someone who persuades others to shred documents under a document retention policy when he does not have in contemplation any particular official proceeding in which those documents might be material."[6]

Similarly, the Advisory Committee Notes to Fed. R. Civ. P. 37(e)[7] make clear that the duty to preserve electronically stored information (ESI) is triggered when litigation is filed, or reasonably anticipated:

> The new rule applies only if the lost information should have been preserved in the anticipation or conduct of litigation and the party failed to take reasonable steps to preserve it. . . . The rule does not apply when information is lost before a duty to preserve arises.[8]

---

4 *See* The Sedona Conference, *Commentary on Inactive Information Sources*, Principle 2, THE SEDONA CONFERENCE (July 2009 Public Comment Version), https://thesedonaconference.org/publication/The%20Sedona%20Conference®%20Commentary%20on%20Inactive%20Information%20Sources.

5 544 U.S. 696, 704 (2005) (internal citation omitted).

6 *Id.* at 708. The Court did not decide whether the Andersen employees did "have in contemplation any particular official proceeding"; instead, the Court reversed and remanded because "the jury instructions [at the trial court] were flawed in important respects."

7 Rule 37(e), which focuses exclusively on ESI, may provide serious consequences for organizations that "fail[ed] to take reasonable steps to preserve" information "that should have been preserved." FED. R. CIV. P. 37(e).

8 2015 Advisory Comm. Note to FED. R. CIV. P. 37(e).

Thus, organizations should not be required to "defend" their disposition of any information that takes place before that duty arises. Indeed, information about the organization's Information Governance program and the organization's disposition practices *before* the duty to preserve arises are typically not discoverable.[9]

> *Illustration:* In a products liability suit, the plaintiff requests discovery regarding the product manufacturer's written Information Governance program, its retention schedule, and a list of relevant information that no longer exists; when that ESI was destroyed; and why that information was destroyed. In responding to the manufacturer's relevance and proportionality objections, the plaintiff makes no showing that the manufacturer violated its duty to preserve ESI after the lawsuit was pending or reasonably anticipated. The manufacturer is entitled to stand on its objections.

Of course, once the duty to preserve has been triggered, organizations must take reasonable steps to preserve relevant ESI, regardless of whether their Information Governance program would otherwise allow or require its disposition. These preservation obligations are discussed in *Comment 1.b.*

Similarly, there may be an obligation to preserve information for government investigations, as discussed in *Comment 1.c.,* and there may be a statutory or regulatory obligation to retain certain information, as discussed in *Comment 1.d.* Lastly, the disposition program should avoid disposing of information that continues to provide operational or other business value to the organization, as discussed in *Comment 2.a.*

Comment 1.b. When designing and implementing an information disposition program, organizations should consider the obligation to preserve information that is relevant to the claims and defenses and proportional to the needs of any pending or anticipated litigation.

A detailed discussion of when the duty to preserve is triggered, and what is required to meet that duty, is beyond the scope of this paper. A general description of those preservation duties is included in *The Sedona Principles*,[10] and a more specific discussion is in The Sedona Conference *Commentary on Legal Holds.*[11]

Information Governance programs must provide for meeting those duties even where the program would otherwise call for disposition of the ESI, such as when the information has met its retention period and no longer provides any business value. Although Information Governance programs do

---

9 *See The Sedona Principles, Third Edition*, *supra* note 3, at 127, Comment 6.c. ("[P]arties should not be required to produce documentation of their discovery processes unless there has been a showing of a specific deficiency in their discovery processes.").

10 *Id.* at 51–53, Principles 5 and 14.

11 *See generally* The Sedona Conference, *Commentary on Legal Holds: The Trigger & The Process*, 11 SEDONA CONF. J. 265 (2010).

not create a preservation duty where it does not already exist, they may come under judicial scrutiny if an organization fails to meet its obligations to preserve ESI for pending or anticipated litigation. As explained by the Advisory Committee Notes to Rule 37(e):

> [C]ourts may sometimes consider whether there was an independent requirement that the lost information be preserved. Such requirements arise from many sources––statutes, administrative regulations, an order in another case, or a party's own information-retention protocols. The court should be sensitive, however, to the fact that such independent preservation requirements may be addressed to a wide variety of concerns unrelated to the current litigation. The fact that a party had an independent obligation to preserve information does not necessarily mean that it had such a duty with respect to the litigation, and the fact that the party failed to observe some other preservation obligations does not itself prove that its efforts to preserve were not reasonable with respect to a particular case.[12]

Thus, even before a duty to preserve arises, selective disposal may still carry risks.[13] For example, if an organization's Information Governance program provides for "selective disposition" of information that would be hurtful if litigation later arises, while allowing for the retention of information that provides little value other than it might help the organization, some courts may consider such an approach as evidence that the organization anticipated litigation when it designed its Information Governance program.

> *Illustration:* Pursuant to its retention schedule, a product manufacturer routinely disposes of product testing results that show the product is unsafe but retains testing results that show the product is safe. The manufacturer later argues that it did not anticipate litigation until it was sued, years after the unhelpful testing results were destroyed. In determining when litigation was anticipated, or reasonably should have been anticipated, the court may consider, among other factors, the "selective disposition" by the organization. In addition, if the court determines that the organization violated a duty to preserve, the court may consider the organization's "selective disposition" in determining whether the organization acted with an "intent to deprive" under Rule 37(e)(2).[14]

---

12 2015 Advisory Comm. Note to FED. R. CIV. P. 37(e) ("The rule does not apply when information is lost before a duty to preserve arises.").

13 *See* Micron Technology, Inc. v. Rambus, Inc., 645 F.3d 1311, 1317–29 (Fed. Cir. 2011) (affirming sanctions for spoliation of evidence plaintiff destroyed in an effort to become "battle-ready" for litigation); *see also* United States *ex rel.* Carter v. Bridgepoint Education, Inc., 305 F.R.D. 225, 240–42 (S.D. Cal. 2015) ("[A] defendant remains free to operate their business in its ordinary course in the absence of the reasonable probability of a certain lawsuit and so long as it does not render data inaccessible purely with the intent of stymying such legal action."); *cf.* FED. R. CIV. P. 37(e) (authorizing the imposition of spoliation sanctions where there is an "intent to deprive").

14 *See* Barnett v. Deere & Co., No. 2:15-CV-2-KS-MTP, 2016 WL 4544052 (S.D. Miss. Aug. 31, 2016) (declining to find sufficient evidence of bad faith and denying sanctions where lawnmower manufacturer's destruction of safety information occurred pursuant to its records policy and before plaintiff's injury, even though defendant had a "'long history of litigating rollover claims'"); *cf.* Phillip M. Adams & Assocs., LLC v. Dell, Inc., 621 F. Supp. 2d 1173, 1191

Information Governance programs should also include a provision to return to "normal" retention/disposition procedures after a duty to preserve ceases. Events during the life of a matter may warrant adjusting the scope of what is preserved. The *Commentary on Legal Holds*[15] observed that it is reasonable for parties to review and revise a legal hold notice when they receive new information that could affect the scope of a legal hold:

> Preservation obligations may expand, or contract, as the contours of claims and defenses are clarified during the pendency of a matter. If the scope of the claims or defenses expands, parties may need to increase their preservation efforts, which may require them to amend their preservation notices. Conversely, when the scope of claims or defenses contracts, the party preserving the information will have an interest in modifying its preservation efforts and notices so that it may resume normal information management procedures for information that is no longer relevant to the claims or defenses.[16]

Prior to the close of discovery, any number of events may provide information that expands or contracts the scope of preservation. These events include reviewing and responding to discovery, interacting with opposing counsel about discovery, and incorporating substantive developments such as amendment, dismissal, or summary judgment. Information gained at such points often clarifies relevant issues, which may warrant adjusting the related legal hold to account for additional or removed issues, claims, defenses, or data sources.

Similar analysis might take place after the close of discovery in light of events such as trial, appeal, or any other significant but not entirely final resolution. Organizations may also consider disposing of ESI that it collected during the litigation but determined not to be relevant. For example, this can include ESI that was culled based on search criteria that have not been challenged or have been agreed to by opposing counsel.

Comment 1.c. When designing and implementing an information disposition program, organizations should consider the obligation to preserve information that is relevant to the subject matter of government inquiries or investigations that are pending or threatened against the organization.

Treatises often combine discussions regarding preservation obligations in civil litigation and investigations because the general tenets are similar.[17] But preservation obligations can differ, because they

(D. Utah 2009) (duty to preserve arose when manufacturer was "sensitized" to product issue and should have had a reasonable expectation of litigation when similar class action claims arose against other manufacturers years earlier).

15 The Sedona Conference, *Commentary on Legal Holds*, *supra* note 11, at 283–84.

16 *The Sedona Principles, Third Edition*, *supra* note 3, at 96.

17 *See* David C. Shonka, *Responding to the Government's Civil Investigations*, 15 SEDONA CONF. J. 1, 8 (2014) ("The principles that govern retention in investigations are the same principles that govern retention in civil litigation: parties are

are often governed by different statutes, court procedural rules, and case law. For many investigations, organizations who receive subpoenas should engage the investigating authority to determine its preservation obligations; however, the agency's own rules, or lack of clear rules, may place parties in a disadvantaged position.

Receipt of a subpoena does not always trigger a preservation duty. For example, if the organization can verify that it has produced the requested information, it may not also need to preserve the information.

Further, the stakes for failing to preserve information may be different for government investigations. For example, parties under a federal investigation may be subject to potential penalties for the obstruction of justice,[18] as opposed to the Rule 37(e) "provisions for sanctioning a party who fails to preserve ESI."[19]

The point at which an organization no longer has a preservation obligation related to an investigation also differs from litigation. The duty to preserve normally ends when the investigation is closed and no further action, including subsequent litigation, is reasonably anticipated. In certain instances, it may be difficult to determine whether an investigation has been completed, leading to the potentially difficult decision of whether to contact the government to discuss the status of the inquiry. Such a discussion could lead to confirmation that a preservation obligation no longer exists but might also lead to renewed focus on a dormant matter. While it may be difficult for an organization to determine when an investigation has been completed, some federal agencies allow, through regulation, for the disposition of information relevant to an investigation if the investigation has been dormant for some specified length of time.[20]

Comment 1.d. When designing and implementing an information disposition program, organizations should consider applicable statutory and regulatory obligations to retain information.

Information retention laws and regulations should be a cornerstone of Information Governance policies. These retention requirements are found in U.S. federal and state statutes, regulations, subregulatory authority, foreign laws[21] and regulations, as well as regulations promulgated by non-governmental regulatory bodies, e.g., the Financial Industry Regulatory Authority (FINRA) in the

---

to take prompt and reasonable, not herculean, steps to preserve and stop the routine destruction and disposition of relevant materials.").

18 *See* 18 U.S.C. § 1505 (providing for up to five years in prison for obstruction of investigatory proceedings).

19 2015 Advisory Comm. Note to FED. R. CIV. P. 37(e).

20 *See, e.g.*, 16 C.F.R. § 2.14(c) (Preservation obligations for Federal Trade Commission investigations end upon notice of closing of the investigation or "after a period of twelve months following the last written communication from the Commission staff to the recipient or the recipient's counsel.").

21 While this section focuses on U.S. retention requirements, organizations need to consider retention requirements in all jurisdictions in which they have employees and do business.

financial sector. These laws are often enforceable by civil and sometimes criminal penalties.[22] Whether specific retention laws apply to an organization depends on a number of factors, including: the organization's structure and industry, the nature of the information created by the organization, and the jurisdiction(s) to which the organization is subject. An organization must ensure its compliance with applicable laws by identifying and complying with requirements that may apply to its information.

While the number of legal retention requirements applicable to an organization may differ greatly based on the factors listed above, some common retention requirements apply to most organizations. For example, even small organizations in unregulated industries must comply with federal and state rules related to tax regulations.[23]

Certain highly-regulated business sectors within the United States must comply with additional retention requirements, generally set forth in federal or state statutes, regulations, or, in some cases, sub-regulatory guidance. Such highly regulated sectors include the financial,[24] energy,[25] and healthcare[26] industries. For example, healthcare providers are required by state laws to retain patient records for various time periods, generally between three and ten years. These requirements vary by state, type of provider, age of the patient, and the patient's condition.[27] Generally, the Health Insurance Portability and Accountability Act (HIPAA) imposes a six-year retention period.[28] Like healthcare providers, banks and financial organizations are also subject to broad retention

---

22 For example, 29 U.S.C.S. § 216 provides for monetary fees up to $10,000 and potential imprisonment for those who violate Labor Department record keeping requirements. 29 U.S.C.S. § 216(a) (2008).

23 *See* 26 U.S.C. § 6001; 26 C.F.R. § 1.6001-1.

24 *See generally* Truth in Savings Act, 12 U.S.C. ch. 44; Equal Credit Opportunity Act, 15 U.S.C. § 1691 *et seq.* (1974); Electronic Funds Transfer Act, 15 U.S.C. § 1693 *et seq.* (1978); Financial Recordkeeping and Reporting of Currency and Foreign Transactions Act of 1970 (Bank Secrecy Act), 31 U.S.C. § 5311 *et seq.*; Truth in Lending Act (Regulation Z), 12 C.F.R. § 226; and 2014 Financial Industry Regulatory Authority.

25 *See generally* Energy Policy Act of 2005, Pub. L. No. 109-58, 119 Stat. 594; 18 C.F.R. § 35; 18 C.F.R. § 284; 18 C.F.R. §§ 366–369; 18 C.F.R. § 368.3; 18 C.F.R. § 375; 36 C.F.R. § 1236; *General Records Schedules Transmittal 23*, U.S. NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (Sept. 2014), https://www.archives.gov/files/records-mgmt/grs/grs-trs23.pdf; *General Records Schedules Transmittal 23*, U.S. NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (Aug. 2014), https://www.archives.gov/files/records-mgmt/grs/grs-trs24.pdf.

26 42 C.F.R. § 422.504(d)(2)(iii); 42 C.F.R. § 482.24(b)(1); 45 C.F.R. § 164.316(b)(2); 45 C.F.R. § 164.530. *See generally* 21 C.F.R.; ALA. ADMIN. CODE r. 420-5-7-.13; 10 N.Y.C.R.R. § 405.10; REV. CODE WASH. (ARCW) § 70.41.190.

27 *See, e.g., Individual Access to Medical Records: 50 State Comparison*, HEALTH INFORMATION & THE LAW, http://www.healthinfolaw.org/comparative-analysis/individual-access-medical-records-50-state-comparison (last updated Sept. 24, 2013).

28 Health Insurance Portability and Accountability Act (HIPAA) of 1996, 45 C.F.R. § 164.316(b)(2).

requirements under a number of regulatory schemes, including the Gramm-Leach-Bliley Act (GLBA) and state statutes.[29]

Many kinds of information about employees are regulated and are subject to explicit minimum retention periods or requirements that information be kept available for audit purposes.[30] Notably, some statutes and regulations require retention of documents that they cover, while other regulations only require retention of documents sufficient to prove required information in an audit. The Sarbanes-Oxley Act (SOX) imposes different record retention requirements on publicly traded companies as opposed to privately held companies.[31] Its requirements relate to work documents underlying any audit or review, insider dealings, and documents related to government inquiries.[32]

PRINCIPLE 2. When designing and implementing an information disposition program, organizations should identify and manage the risks of over-retention.

Comment 2.a. Information has a lifecycle, including a time when disposal is beneficial.

Like everything else, information has a lifecycle that begins with its creation or receipt and ultimately ends with its disposal. The length of that lifecycle and the course it takes depend on each recipient's use for the information. Thus, the creation of information marks the beginning of its lifecycle for the author, while the receipt of the information marks the beginning for each recipient. The end of the lifecycle depends on the use for the information. And, of course, these uses vary greatly among recipients and among types or categories of information. For example, the useful lifecycle for some types or categories of information varies (e.g., employee contact information is principally useful to most users only for as long as that employee remains with the organization—whether two weeks or 40 years); the utility of other information is transient (e.g., the usefulness of the content of an email may end when it is read or assimilated into larger work); still other information may have a defined life (e.g., information subject to a regulatory disposition requirement); and some information may have permanent value (e.g., information of historical significance).

---

29 *See, e.g.*, Gramm-Leach-Bliley Act, Pub. L. No. 106–102, 113 Stat. 1338 (1999); MCKINNEY'S CONSOLIDATED LAWS OF NEW YORK, BANKING LAW § 128; ADVISX RISK MANAGEMENT, RECORD RETENTION SCHEDULE FOR BANKS (Feb. 19, 2017).

30 For example, job applications, job postings, personnel records, payroll records, reasonable accommodation requests, and immigration records are subject to records requirements under the Americans with Disabilities Act (ADA), the Age Discrimination in Employment Act (ADEA), Title VII of the Civil Rights Act of 1964, the Fair Labor Standards Act (FLSA), and the Immigration Reform and Control Act (IRCA). Other employee records may be subject to the Fair Credit Reporting Act (FCRA) of 1969, 15 U.S.C. § 1681 (seven-year reporting period); the Lilly Ledbetter Fair Pay Act of 2009; ERISA; and OSHA.

31 Sarbanes-Oxley Act of 2002, Pub. L. 107–204 § 802, 116 Stat. 745.

32 *Id.*

The lifecycle of information thus depends on the context in which it is created and used. Effective (and defensible) Information Governance programs require organizations to figure out the useful life of all types of information and then set meaningful retention periods for each type. Such decisions should be based on informed business judgments and may include factors other than the immediate "business need" for the information. For example, some information may not be actively used by the organization for ongoing business operations but may have long-term business benefits (e.g., to safeguard the design plans for certain products or to ensure an orderly transfer of knowledge to successor employees or successor owners of the business).

Information not subject to legal or regulatory obligations should be retained only as long as justified by its operational value to the organization. Determining the operational value of information involves a cost/benefit analysis. The costs at issue are not simply the storage costs to maintain the information but include the risks inherent in retaining the information longer than necessary. This analysis can represent a significant cultural shift in how the organization previously looked at the retention of information. As organizations grapple with the necessary cultural shift toward disposition of stale information, there can be a tendency to overstate the business value of retention, without full consideration of the increased costs and risks associated with retained information. Operational value of information can be evaluated based on its value to: (1) business function and corporate governance; (2) internal audit and compliance; (3) potential (but not yet "reasonably anticipated") litigation; and (4) contract requirements.

1. Business Function and Corporate Governance

Much information has operational value for a relatively brief time; some of it is stale immediately after it is created. Day-to-day business communications and operational documents may only be required for that day. Other documents may be required for years, such as specifications for a long-term project, or active contracts with multi-year terms. Corporate governance documents generally provide permanent value to an organization, as they are foundational. The operational value of information can be ascertained by working with business departments and custodians who create and use the information and assessing how often information types tend to be accessed after they are created.

2. Internal Audit and Compliance

Similar to legal requirements, organizations may create internal compliance programs as part of a corporate governance program. Such policies may require retention of information that exceeds legal requirements, and audits of compliance may require availability of additional supporting documents and information. Such categories of information need to be retained for as long as they are required by the compliance program.

3. Potential (but not yet "reasonably anticipated") Litigation

Beyond preservation requirements for existing or anticipated litigation, some organizations may elect to retain information that is not subject to a preservation requirement but could be valuable in

future litigation that is not yet "reasonably anticipated." For example, manufacturers may opt to retain records documenting safety testing of their products, because either experience dictates, or industry practices show, that in the event they face a lawsuit for an injury, this information could be of value if litigation ensues. Organizations often retain documents related to research and development efforts in case they need to defend a challenge to a patent. Retention based on business needs regarding potential litigation should be tailored to the organization's litigation risk profile and should be carefully balanced against the risks and costs of retaining the information beyond its business function. In general, such information should be retained only for as long as the potential litigation is a risk.

4. Contract Requirements

Many organizations are parties to contracts that require retention of information for a specified period and then require disposition. Such arrangements may appear in retainer agreements between parties who exchange proprietary information about their organizations or sensitive private information about their employees and customers.[33]

Comment 2.b. To determine the "right" time for disposal, risks and costs of retention and disposal should be evaluated.

Information that is not subject to a legal, regulatory, or business retention obligation should be disposed of as soon as the cost and risk of retaining the information outweighs the value of retaining the information. Accurately determining information lifecycles and implementing an orderly disposition process are complex undertakings. An organization should know its information, its information systems, and its comfort with various levels of risk. A variety of teams within an organization[34] must collaborate in order to achieve successful Information Governance design and implementation. Organizations can and do benefit from appropriately disposing of information when it reaches the end of its legally required or functionally useful life. Some of those benefits include: (1) increased productivity and efficiency; (2) reduced storage costs; (3) improved legal compliance; (4) reduced discovery costs and risk; and (5) enhanced data privacy and security benefits.

---

[33] Such provisions may also appear in case management orders and protective orders.

[34] For example, the IT team usually focuses on information storage and potentially retrieving inadvertently deleted information. The Information Governance team focuses on enhanced and appropriate information accessibility, information lifecycles, and appropriate disposal at the predetermined end of those lifecycles. The security team is primarily concerned with restricting access to data to only appropriate personnel and preventing breaches. Somewhere in the mix are the lawyers, who may be primarily concerned with the legal compliance of the policies the organization adopts; the stakeholders, who primarily want quick access to the information they need and may not particularly care about where that information ends up; and the directors and managers who must balance the benefits and risks of whatever course the organization should take. All these groups need to collaborate when adopting and implementing any Information Governance program and information disposition program.

1. Increased Productivity and Efficiency

To show the waste of resources and lost productivity that results from keeping information beyond its required retention, an organization need only consider the time that individual employees waste in searching their own files for information they have previously prepared or read and stored. Almost anyone who uses a computer regularly can relate to such situations. If these individual experiences are multiplied by the number of employees who use computers in a given organization, it is possible to grasp the likely scope of the problem. This waste is an economic loss that has two aspects: first, that which results from the inability to promptly find information when it is needed; and second, that which results from trying to isolate the correct information from among the mass of information in the system. The first of these relates to information organization and management; the second relates to records disposition and a failure to dispose of unneeded information.

In addition to the issues presented by individual employees and their own filing and retention habits or processes, similar issues are raised by corporate- or even division-level systems that collect and retain information. If allowed to accumulate, the volume of this information can quickly aggregate into petabytes or more of information. Even for modern computing systems, it takes much more time to process data when it contains large volumes of unneeded information.[35] Simply, being able to find the right information quickly results in greater efficiency and higher productivity.

2. Reduced Storage Costs

Although storage costs are relatively inexpensive and have for a long time been declining, information is accumulating rapidly, and in some cases exponentially. Moreover, storage costs accrue for the duration of the information storage: whether one year, two years, or indefinitely. To the extent the Information Governance process properly categorizes information, it can be managed efficiently from the beginning to the end of its lifecycle. These efforts reduce ever-increasing, and unnecessary, storage costs by limiting data growth of systems in use, as well as reducing the burdens of retired legacy systems, from which data retrieval can be expensive.

3. Improved Legal Compliance

In weighing the benefits of an information disposition program, organizations should consider their legal obligations to dispose of information. In this regard, there are several situations in which an organization may be obligated to dispose of information, such as where the information is subject to (a) statutory or regulatory mandates (e.g., the Federal Trade Commission (FTC) Disposal Rule, the HIPAA Privacy Rule, and COPPA[36]); (b) court orders that compel the destruction of information

---

[35] Large data volumes can greatly impact the performance and user experience with systems—even crippling the system in some circumstances.

[36] *See* Children's Online Privacy Protection Act (COPPA), 16 C.F.R. § 312.10 (Oct. 21, 1998) (A company is allowed to retain children's personal information "for only as long as is reasonably necessary to fulfill the purpose for which the information was collected." After that, the company must delete it using "reasonable measures to ensure it's

(e.g., certain protective orders governing discovery information following litigation); and (c) contractual agreements that require the parties to dispose of information at a specified time. Depending on the circumstances, any failure to dispose of information subject to a disposition requirement may result in fines, civil penalties, litigation sanctions, contempt citations, or even damages claims, not to mention attendant litigation expenses. These punitive results can be quite severe.[37]

In addition to the three situations highlighted in the previous paragraph, some organizations should also pay attention to information disposition requirements imposed by foreign law. Although a discussion of global privacy laws and policies is beyond the scope of this paper, it is worth noting that some nations take a far more restrictive view about the use of personal information than the United States. For example, in the European Union (EU), privacy has been treated as a fundamental human right for many years. Laws restrict the use of personal information and generally require disposition after its intended use, as exemplified by the General Data Protection Regulation (GDPR), effective in EU countries as of May 2018.[38] Among other things, that law restricts the use of personal information, heavily regulates its "onward transfer," establishes disposition and breach notification requirements, requires erasure or the "right to be forgotten" for personal information, and imposes substantial penalties (up to 4% of a firm's global turnover) for violations of the law. Notably, EU regulators assert that the law has extraterritorial effect, which could mean that an organization that properly collects information in the EU and transfers it to the United States may be liable in the EU for losses occurring in the United States, even if the losses are caused by a later recipient of the information. While the scope and reach of the GDPR (and other nations' similar privacy laws) are at this time not firmly settled, organizations may wish to consider the possibilities when setting up information disposition programs.

4. Reduced Discovery Costs and Risks

While a major goal of the 2015 amendments to the Federal Rules of Civil Procedure was to address serious problems associated with the impact of the expanding volume of electronically stored

---

been securely destroyed."). On May 31, 2018, the FTC clarified (i) when children's personal information must be deleted and (ii) how the requirement applies; as well as recommended that covered companies review their information retention policies to ensure they are in compliance. *See* Jared Ho, *Under COPPA, data deletion isn't just a good idea. It's the law.*, FEDERAL TRADE COMMISSION (May 31, 2018), https://www.ftc.gov/news-events/blogs/business-blog/2018/05/under-coppa-data-deletion-isnt-just-good-idea-its-law?utm_source=govdelivery.

37 For example, HIPAA Privacy and Security Rule violations carry maximum civil penalties of $50,000 per violation, with an annual maximum of $1.5 million, and potential criminal penalties including imprisonment. *See* 45 C.F.R. 160.404.

38 *See* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119/1) [hereinafter GDPR], https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN. *See also* Article 29 of Directive 95/46/EC Data Protection Working Party, https://iapp.org/resources/article/all-of-the-article-29-working-party-guidelines-opinions-and-documents/.

information in civil discovery,[39] over-retention and improper or ineffective disposition efforts still pose a significant risk and drive up discovery costs. The more information an organization maintains and the longer information is retained, the more it will cost to identify, preserve, search, and produce that information in the event of litigation, investigation, or any other instance of compulsory process.[40] Also, if an organization does not properly account for preservation requirements in its disposition processes for systems subject to automatic deletion, the organization may be exposed to litigation sanctions or other penalties.

a. Likelihood and Size of Potential Discovery

When conducting a discovery[41] response risk analysis in the context of information disposition, an organization should start by reviewing its overarching risk portfolio. It should assess the nature of its business, the types of information maintained, and its litigation/investigation/audit history to predict the likelihood of various types and costs of future discovery responses, and the types of information affected by those instances. This analysis should help the organization identify information types most likely to be subject to discovery and structure disposition practices accordingly.

For example, consider a small online cloud-based service provider. The organization does not have a physical product and its product liability exposure is low. It has a small workforce so there is a risk of employment litigation, but no risk of large class action employment lawsuits. Based upon industry experience for similarly sized organizations, the main litigation risk is likely to be in contract or intellectual property disputes. Therefore, when determining how litigation risk impacts its disposition practices, the first priority could be information relevant to breach of contract and intellectual property litigation, including but not limited to trade secret claims.

Consider also a small technology company in the business of creating mobile healthcare apps with a dual purpose: (1) serving the individual users by providing general information and allowing users to track their personal health trends through individual data input; and (2) using that input to generate big data in order to identify statistically significant trends, in turn serving the individual users as well as the various healthcare providers invested in the company. This company has the same considerations as the cloud-based service provider referenced above, but also has a variety of additional data privacy and security concerns because the end users enter personal information into the mobile apps. Other concerns might include investigations by state and federal agencies in the healthcare and digital privacy and security realms. These additional concerns should be taken into account when structuring a comprehensive information disposition policy and procedures for implementing that policy, including cessation of routine disposition when litigation, investigation, audit, or other compulsory process instances arise.

---

39 *See* JOHN G. ROBERTS, JR., 2015 YEAR-END REPORT ON THE FEDERAL JUDICIARY 5 (Dec. 31, 2015), https://www.supremecourt.gov/publicinfo/year-end/year-endreports.aspx.

40 *E.g.*, third-party subpoena, civil investigative demand, regulator request, or audit.

41 The discovery process can involve litigation as well as other compulsory process, such as a subpoena from a government agency or from a litigating party.

b. Potential Costs of Discovery, Given Data Volumes and Types

While the nature and scope of information that must be preserved when discovery instances arise is case-specific, making it impossible to calculate the exact costs related to any such circumstance, studies have analyzed typical discovery costs from preservation through document production.[42] These studies may help organizations conduct informed risk assessments as discussed above, as they indicate that preservation and production costs (internal and actual out-of-pocket), may be managed by better disposition practices. Such cost reductions may include:

(1) less cost to track down information sources that may contain relevant information;

(2) less cost searching for and analyzing old and inactive legacy information sources to determine whether they contain relevant information;

(3) less cost implementing and monitoring preservation obligations;

(4) smaller volume of information to collect and process into review-ready format;

(5) less time and effort spent reviewing documents; and

(6) fewer documents to produce.

Ever-developing eDiscovery technology, such as Technology Assisted Review (TAR), may help to defray costs, but that does not serve as a substitute for a comprehensive information disposition policy. First, reduction elements 1–4 above are not affected by the use of this type of technology. Second, many cases and investigations are not suitable for the use of advanced technologies because the matter is simply too small to justify the cost or use of advanced technologies but may nonetheless consume significant discovery resources. Third, machine identification of relevant documents works best and most efficiently on document sets that begin with a sufficient percentage of responsive documents. Finally, even when TAR is used, other review costs can still be expensive, such as review for privilege and other sensitive information.

c. Risks Associated with Discovery and Improper Disposal

Organizations may not be sanctioned in litigation for failing to produce information that was properly disposed of before litigation was reasonably foreseen, and an organization cannot be found to have obstructed justice for failing to produce information properly disposed of before an investigation commenced. In *Solo v. United Parcel Service Co.*, the producing party had already disposed of information sought in discovery by deleting it from its active information location. While the

---

[42] *See, e.g.*, William H.J. Hubbard, *Preservation Costs Survey Final Report*, ELECTRONIC DISCOVERY LAW (Feb. 18, 2014), https://www.ediscoverylaw.com/files/2014/02/Hubbard-Preservation_Costs_Survey_Final_Report.pdf; Nicholas M. Pace & Laura Zakaras, *Where the Money Goes: Understanding Litigant Expenditures for Producing Electronic Discovery*, RAND INSTITUTE FOR CIVIL JUSTICE (2012), https://www.rand.org/pubs/monographs/MG1208.readonline.html.

information could have been produced from backup tapes, the court found that a "valid business reason" existed for the deletion and did not require "extraordinarily burdensome" production of the information.[43]

Counsel should actively engage their client in a discussion about the creation and implementation of an Information Governance program and, in particular, information disposition activities, because those may affect how the organization complies with its discovery obligations. For example, pursuant to Rule 26(g)(1) of the Federal Rules of Civil Procedure, an attorney who signs a discovery response certifies that the lawyer has made a reasonable effort to assure that the client has provided the documents available to the client that are responsive to the discovery demand. If the certification violates the rule "without substantial justification," under Rule 26(g)(3) the court "must impose an appropriate sanction on the signer, the party on whose behalf the signer was acting, or both." Therefore, the risk of sanctions for improper disposal extends to counsel who make such representations, their clients, or both.

5. Enhanced Data Privacy and Security Benefits

An organization must be concerned about the security of its information, and particularly its commercial, financial, employee, and proprietary information, no matter its age or format. Proper, timely, and routine disposition yields less information. It is cheaper and easier to protect less information than more. Also, in the event of a loss or breach, the cost of information recovery and the burden of notifying interested parties decrease when the volume of information lost is smaller and the sensitivity of compromised data is known.

Indeed, a security breach[44] can cause substantial harm for any organization. According to a 2016 study sponsored by IBM and conducted by the Ponemon Institute, the average cost of a single information breach was roughly $4 million.[45] The average cost paid for each lost or stolen record

---

43 2017 WL 85832 (E.D. Mich. Jan. 17, 2017); *cf.* United States *ex rel.* Guardiola v. Renown Health, No. 3:12–cv–00295–LRH–VPC, 2015 WL 5056726 (D. Nev. Aug. 25, 2015) (finding a party's deliberate reliance on disaster recovery tapes for preservation reflected failure to adopt "a sensible email retention policy" so the organization could not be excused from its large burden of compliance).

44 While this section focuses on information breach, organizations face non-breach security risks as well. Most state information breach statutes cover the unauthorized access or acquisition of personal information ("PI"). *See, e.g.*, CAL. CIV. CODE 1798.82; MASS. GEN. LAWS ch. 93H; TENN. CODE ANN. § 47-18-2107. If information is compromised, but no PI is acquired by an unauthorized person, there might not be a "breach" but the security has still been affected. For example, if an organization's information is attacked in a denial-of-service attack, the information may not have been "breached" under most statutory definitions, but the organization's information security has been compromised nonetheless, potentially yielding a variety of business risks and costs.

45 PONEMON INST. LLC, 2016 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS 1 (June 2016), http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=sel03094wwen [hereinafter PONEMON STUDY] (The study did not include "mega breaches," or information breaches of more than approximately 100,000 compromised records, in its average cost numbers.).

containing sensitive or confidential information was $158 per record.[46] Cost components include: (1) detection and escalation;[47] (2) notification;[48] (3) post-breach management and remediation;[49] and (4) lost customers.[50] These costs correlate to the volume of information breached—the more information lost, the greater the attendant costs.[51] The costs and risks of a breach vary by industry.[52] Because of additional privacy and security requirements, heavily regulated industries such as healthcare and finance[53] have information breach costs well above the $158 per record average.[54] Organizations operating in the European Union may face similarly heightened information privacy laws, as well as the related heightened risk and costs.[55]

For these reasons, organizations have a strong incentive to limit information breach exposure by reducing the amount of information retained and employing secure and defensible disposition practices. Organizations with less data can more easily protect their data at less cost. Regulatory agencies are now recommending that organizations, as part of their cybersecurity program, have policies for the secure disposal of information that is not required to be retained by law or regulation.[56] The FTC also recommends that organizations consider data minimization (i.e., limiting the collection of consumer data, and retaining that information only for a set period of time, and not indefinitely) to reduce the attractiveness of those repositories to data thieves, the harm done to consumers when breach occurs, and the risk of use of the data in ways not consistent with the data's intended use.[57]

---

46 *Id.*

47 *Id.* at 18.

48 *Id.*

49 *Id.*

50 *Id.* at 19.

51 *Id.* at 15.

52 *Id.* at 2. *See also* VERIZON, 2016 DATA BREACH INVESTIGATIONS REPORT 3–4 (2016), http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf.

53 For example, recall the breaches at Target and BJ's Wholesale. *See, e.g.*, Peter Cooney & Supriya Kurane, *Target agrees to pay $10 million to settle lawsuit from information breach*, REUTERS (Mar. 19, 2015), https://www.reuters.com/article/us-target-settlement/target-agrees-to-pay-10-million-to-settle-lawsuit-from-data-breach-idUSKBN0MF04K20150319; *In re* BJ's Wholesale Club, FEDERAL TRADE COMMISSION (Sept. 23, 2005), https://www.ftc.gov/enforcement/cases-proceedings/042-3160/bjs-wholesale-club-inc-matter.

54 PONEMON STUDY, *supra* note 45.

55 *GDPR Key Changes*, EU GENERAL DATA PROTECTION REGULATION, https://www.eugdpr.org/key-changes.html (last visited April 8, 2018).

56 *See* NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES, 23 N.Y.C.R.R. § 500 (2017), Section 500.06 Audit Trail and Section 500.13 Limitations on Dara Retention (requirements for audit trails and annual compliance reports by Chief Information Security Officer).

57 *See* FTC STAFF REPORT, INTERNET OF THINGS, at iv (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

Disposition practices should protect against a variety of potential security breach incidents, including, but not limited to, malicious and targeted external cyber attacks, phishing attacks, malware, social engineering, employee error, unique vulnerabilities of legacy storage systems that are not updated with security patches, and malicious actions by insiders.[58] Therefore, when developing a secure information disposition plan, organizations should not only focus on the physical destruction of hard copy records and computer hardware, but also pay particular attention to how information is stored, transferred, and ultimately destroyed. This includes in-house systems as well as storage and other services provided by third parties and cloud service providers. As more organizations move all or part of their information infrastructure offsite or into the cloud, the number of possible information breach points increase. When instituting an information disposition plan, organizations should make sure third parties, including cloud service providers, who store or have access to the organization's information also comply with that disposition plan. This involves negotiating for appropriate disposition and security language in contracts and auditing/confirming that if the organization disposes of information based on its Information Governance policy, a third party will not be holding onto a copy of that information, unbeknownst to the organization.

PRINCIPLE 3. Disposition should be based on Information Governance policies that reflect and harmonize with an organization's information, technological capabilities, and objectives.

Comment 3.a. To create effective information disposition policies, organizations should establish core components of an Information Governance program, which should reflect what information it has, when it can be disposed of, how it is stored, and who owns it.

First, the organization should establish at least the following Information Governance components, which reflect what information it has and how processes apply to that information:

1. Classification

The "what" of the process: An organization should know what types of information are stored before determining appropriate retention periods and procedures. Defining information categories into a taxonomy is a prerequisite to organizing information according to the information that they contain. Category definitions need to balance the ease of use of broadly defined records categories against different needs that could be addressed through narrowly defined records. Categories can be defined based on criteria such as the content of the documents, the business group or employee that created it, where the record is stored, and the type of file.

---

[58] *See* VERIZON, *supra* note 52, at 7–8, 17.

2. Retention Periods

The "when" of the process: Retention periods should set how long each classification of record should be retained and when it should be eligible for disposition. Historically, many organizations created only minimum periods for records retention, yet did not specify whether information should be disposed of after the retention period. Retention periods can be based on criteria such as date created, last date accessed, and a set passage of time after an event (e.g., a product release, a contract expiration, or departure of an employee).

Without retention schedules for different categories of data, organizations often can only dispose of information that is older than a single maximum retention period that is long enough that it can be applied to all information. While better than nothing, this likely results in massive over-retention and failure to realize many benefits of an effective information disposition policy.

3. Knowledge of IT Infrastructure

The "how" of the process: An organization's Information Technology (IT) infrastructure dictates what mechanisms are available to delete information. Disposition processes depend on where information and copies of information reside, what options exist to preserve and delete information, and whether information deletion can or should be automated. If the Information Governance team determines that existing IT infrastructure does not support desired processes, the organization will need to consider updating its available technology.

4. Ownership

The "who" of the process: As described below, every organization needs personnel for documentation, oversight, and maintenance of information disposition as part of the Information Governance program. Designated personnel can provide oversight, help identify potential risk, provide flexibility should objectives change, and may provide valuable metrics regarding performance and efficiency.

Comment 3.b. An organization should understand its technological capabilities and define its information objectives in the context of those capabilities.

To create a successful disposition policy, organizations should define their information objectives. In addition, they should determine technological capabilities, so they can make decisions about their policies that reflect those circumstances.

Where the available technology limits the achievability of information objectives, the organization should decide whether to revise the objectives, update the technology, or both. Technological capabilities affect key decisions when designing a disposition program, such as the possibility of automated records management, how broadly to define records categories, and how policies will be applied to records.

1. Automated Records Management

Automation of ongoing retention and disposition policies may create a more reliable and consistent process than reliance on employees' manual efforts. Therefore, organizations may evaluate the organization's existing information management technologies, and consider new technologies to automatically retain, delete, preserve, and archive information, and facilitate searching.

Selection of records management tools should reflect business needs, litigation portfolio, information volume, and IT infrastructure. An organization should maintain documentation of how each information management tool is used to comply with its information processes.

2. Records Categories

There are many ways to look at organizing records. In deciding which type of classification system to use, the organization should determine the relative risks and benefits. Granular classification systems enable precise document control, make retrieval of needed information easier, and minimize the risk that the organization will accumulate records that raise liability concerns. Conversely, big bucket classification systems will be easier to understand (increasing the likelihood of compliance) and administer, but increase the risk associated with the accumulation of unwanted and useless records.

3. Policies for Different Groups

Information disposition policies can be implemented across the entire organization, or they can be applied differently to different groups, such as offices, departments, or job functions. When making these decisions, organizations should consider what information is stored by each of these groups and how that information tends to flow within the organization.

4. Location of Records

In some cases, it is most convenient to classify information based on its location, either because a data source is configured to store a certain type of information, or because employees have directed a certain type of information to be stored there. For example, email records are often kept on email servers along with other emails, even if they relate to different subjects. The same may be true for voicemail. In addition, employees may use shared drives and folders to store related files, such as all marketing materials or all executed contracts.

Thus, organizations can consider retention periods based on the location of information. For example, an organization may decide to automatically delete all email in 45 or 60 days, while creating a process to copy some emails or attachments to other locations for longer retention or preservation when needed.

5. Legal Hold

An organization must determine whether and how it will continue with its information disposition policies when implementing a legal hold and how it will return to its disposition procedures when the hold is lifted. When implementing a legal hold, an organization's options could include: (1) suspend deletion for the entire organization, or part of the organization; (2) suspend deletion for information from specific employees; or (3) continue all deletion but find an alternative way to effectively segregate and preserve relevant information. The cost of this decision may have a wide-ranging effect on the organization.[59] At one end, the cost of suspending all disposition may be minimal; but the cost resulting from excessive accumulation of unnecessary information may be substantial. At the other end, the need to carefully tailor preservation efforts and take extra steps to save only the most relevant information will likely make the cost of complying with the legal hold more expensive; but the overall information disposition program will continue unhindered.

The approach selected will also affect how the organization will return to its disposition program when a legal hold is lifted. The approach will want to ensure that previously preserved information that is now eligible for disposition will be deleted; while information still within its retention period (or on another legal hold) can be retained for the duration of that period, and then deleted. The organization will benefit if its disposition program includes a process for dealing systematically with information no longer subject to legal holds.

As a practical matter, organizations may choose to incorporate legal hold assessment into their disposition policies. Assessment actions could include: (1) instituting a procedure that notifies IT and suspends automatic deletion on relevant custodian and production systems as soon as the organization is aware of the preservation obligation; or (2) incorporating preservation checks into the disposition process, giving users the ability to confirm that information is not subject to a preservation obligation before it is destroyed.

6. Disposition by Business Partners, Contractors, Vendors, and Cloud Services

Information disposition polices could be viewed as ineffective if a third party continues to hold copies of an organization's information past its established retention period. Whenever organizations will be exchanging information with outside providers or partners, they should determine the degree of control they maintain over their own information after these exchanges. To the extent possible, they should ensure continued control to implement retention and deletion policies. Third parties should be vetted to determine whether they can comply with the organization's requirements for preserving and disposing of its information. The organization should ensure it maintains the control it needs through its third-party contracts. When terms of service govern the relationship, such as with a cloud information service, those terms should be monitored for periodic changes.

---

[59] For example, the organization might move relevant emails into an archive folder before an auto-delete function disposes of them.

Many cloud service providers are in business to provide convenient storage for their customers and have no particular understanding of an organization's records management practices and retention or disposition practices.[60] To avoid losing the benefits of cloud storage, or having them partially or wholly offset by the loss of control over the organization's information, organizations should carefully review cloud service contracts before entering into them. Whenever possible, they should consider engaging providers who will follow the organization's Information Governance policies. If that is not possible, an organization may consider the feasibility of encrypting information before it is stored in the cloud, and then disposing of the decryption keys at appropriate times, thus achieving "virtual" if not actual disposition.[61]

7. Backups and Disaster Recovery Systems

Business continuity and disaster recovery systems, including backup tapes,[62] pose the potential for significant burden and delay in discovery. While case law and The Sedona Conference support the concept that backup tape rotation cycles do not have to be suspended in anticipation of the typical litigation,[63] they may be subject to preservation and become a source for production if they are the sole source of relevant information, are reasonably accessible, and are proportional to the needs of the case.[64]

Like other forms of information storage, the longer an organization maintains secondary copies of information as part of its backup or disaster recovery process, the greater the risk that the information will need to be preserved, searched in future litigation, or subject to a security breach. Searching for information takes time and resources, and searching for information in a difficult to

---

60 *See* ARMA INTERNATIONAL, GUIDELINE FOR OUTSOURCING RECORDS STORAGE TO THE CLOUD (2010), https://www.abraxasworldwide.com/wp-content/uploads/2018/01/Cloud-Storage.pdf.

61 This alternative is not an ideal solution. For a further discussion of encryption, *see* The Sedona Conference, *Commentary on Privacy and Information Security: Principles and Guidelines for Lawyers, Law Firms, and Other Legal Service Providers*, 17 SEDONA CONF. J. 1, 25–26 (2016).

62 While more and more companies are moving from tape to disk or cloud-based solutions, the discovery issues that tapes raise can hold true for other types of recovery systems, regardless of medium.

63 *See* Zubulake v. UBS Warburg, 220 F.R.D. 212, 218 (S.D.N.Y. 2003) (*"Zubulake IV"*) (As a general rule, a "litigation hold does not apply to inaccessible backup tapes" which "may continue to be recycled."). *See also The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production, supra* note 3, at 113, Principle 5, cmt. 5h ("Absent good cause, preservation obligations should not extend to disaster recovery backup tapes created in the ordinary course of business.").

64 *See, e.g.,* Pension Comm. of the Univ. of Montreal Pension Plan. v. Banc of Am. Sec., LLC, 685 F. Supp. 2d 456, 479 n.99 (S.D.N.Y. 2010) (abrogated on other grounds):

> A cautionary note with respect to backup tapes is warranted. I am not requiring that *all* backup tapes must be preserved. Rather, if such tapes are the *sole* source of relevant information (*e.g.,* the active files of key players are no longer available), then such backup tapes should be segregated and preserved. When accessible information satisfies the requirement to search for and produce relevant information, there is no need to save or search backup tapes.

access system such as backup tapes compounds that burden. An effective way to lower the risk of unique information residing on backups is to use short rotation cycles for backups. Backup rotation cycles (both tape and virtual backups) should be no longer than is necessary to ensure business continuity. Moreover, information storage policies, procedures, and systems should be designed to ensure the availability of business-critical information such that business continuity and disaster recovery systems can be used only in the event of a system failure and not to recover information accidentally deleted in the ordinary course of business.

8. Enforcement

Monitoring compliance is key to the success of an Information Governance program. An audit process is recommended to assess whether records are being managed as anticipated and employees are following policies. For example, an organization may periodically report on information volume metrics, sample certain information sources, and interview business operations employees regarding document management practices. When noncompliance or weaknesses in established policies are discovered, such issues should be appropriately addressed. The policy should state what methods will be used for auditing, who has enforcement authority, and what steps (including penalties) the organization should take to address noncompliance.

While an organization is not legally required to document its information disposition processes and events, documentation can support enforcement and facilitate auditing of whether information has been deleted.[65] For example, policies can describe how legal holds are implemented, including use of any legal hold software. Any significant ad hoc deletion events, such as a "clean up" event or information destruction by a third party, may be recorded into a disposition log. Documentation of audit procedures, and results of audits, may further strengthen the credibility of an organization's claims that it follows its written policies. Similarly, employee training in compliance with Information Governance policies may provide key evidence of the defensibility of an organization's information disposition and preservation policies and procedures.

9. Maintenance

Organizations should periodically reassess their information, technology, and objectives, and update their Information Governance programs to address changing circumstances related to disposition. To stay current, companies should conduct regular reviews of legal, operational, and technological developments that may concern the organization's Information Governance program. Organizations may also uncover gaps in their intended procedures through the audit process. To keep up with

---

[65] For example, if relevant information is no longer available when litigation arises, documentation of information disposition policies and practices could be used to demonstrate that the information was properly deleted as well as the timing of the deletion. In the event of alleged spoliation, courts may look to policies and procedures for retention and preservation to determine the culpability of a party. *See* Barnett v. Deere & Co., No. 2:15-CV-2-KS-MTP, 2016 WL 4544052 (S.D. Miss. Aug. 31, 2016) (denying sanctions where lawnmower manufacturer's destruction of safety information occurred pursuant to its records policy and before plaintiff's injury, even though defendant had a "'long history of litigating rollover claims'").

evolving needs, organizations may need to update disposition policies, disposal procedures, or adopted technologies.[66]

In addition to regularly occurring reviews, organizations should identify events that may lead to ad hoc reviews designed to maintain or improve information disposition. For example, before new technologies are deployed, they should be subject to an onboarding process that determines whether they are compatible with the existing Information Governance program.[67]

---

[66] Consider how email, instant messaging, and most recently team collaboration tools (e.g., Slack) brought with them unique Information Governance challenges.

[67] Specifically, new applications can be evaluated to determine whether: (i) the new applications support automatic disposal; (ii) the disposed of information could still be recovered; and (iii) there is a process for preserving information if subject to a legal hold. This assessment should occur whether deployed within the organization or hosted by a third party.

III. INFORMATION DISPOSITION CHALLENGES

While information disposition is important and increasingly necessary for organizations, its practice is not always straightforward. Information disposition can especially create challenges in the following areas:

A. Unstructured Information

Even for organizations that have implemented sound document retention and information disposition policies and procedures, unstructured information presents difficult challenges. Unstructured information is often information that predates the implementation of current document management processes. While new information may be created and organized in a way that enables the organization to manage the information through its lifecycle, unstructured information, by definition, lacks structure so it is much more difficult for the organization to manage that information. Media and format obsolescence can create access problems with legacy systems, along with increased discovery costs due to missing hardware, lapsed software licenses, or software that does not work on current operating systems. An organization should conduct a due diligence review to identify all active and inactive legacy information sources, determine the information contained in them, and assess what information needs to be retained and what can be deleted.

Related data challenges may also include dealing with inactive information sources, as described in The Sedona Conference *Commentary on Inactive Information Sources*. Inactive data sources include: (i) data that is orphaned, for which no one in the organization is able to provide insight on its content or historical use; (ii) legacy data, which is no longer compatible with the organization's systems or programs; and (iii) dormant data, which is no longer used or accessed. As with all information, inactive information should be disposed of when it no longer meets legal retention requirements or business needs.[68]

In some cases, organizations will not know whether a source of inactive information is subject to retention requirements. In such cases, the organization should consider the potential costs of identifying information subject to retention, as well as circumstances that make the source likely or not likely to contain such information subject to retention, and the potential importance of such information to the organization. This analysis may involve interviewing employees who may have knowledge of the information, reviewing documentation regarding the source, or performing statistical sampling.[69]

---

[68] The Sedona Conference, *Commentary on Inactive Information Sources*, THE SEDONA CONFERENCE (July 2009 Public Comment Version), https://thesedonaconference.org/publication/The%20Sedona%20Conference®%20Commentary%20on%20Inactive%20Information%20Sources.

[69] *See*, *e.g.*, Solo v. United Parcel Service Co., No. 14-12719, 2017 WL 85832 (E.D. Mich. Jan. 10, 2017) (allowing possibility of sampling relevant data in context of a burdensome discovery request).

B. Mergers and Acquisitions

Mergers and acquisitions can result in the acquisition of another organization's data policies and practices including record retention plans (or lack thereof). The impact on the original organization's record retention policies and procedures can be significant and complicated. Acquisition of an organization with poor or ineffective Information Governance policies can create significant risk until strong processes can be applied to the information. The acquiring entity should already have its own Information Governance processes in place, but it will need to assess whether those processes are a good fit for the information from the acquired entity. Organizational knowledge of that information may be lost if employees leave, creating additional risk and making assessment of the information difficult.[70] Merging the two entities' document retention policies and practices should be done carefully and deliberately, and should ideally involve a collaborative approach including personnel from both entities.

C. Departed, Separated, or Former Employees

A retention policy should outline next steps for managing information of employees who leave the organization. Former employees' records should generally be retained in accordance with records retention policies but may need to be held longer depending on the circumstances of the departure. For example, an organization may retain information from employees who present a higher risk of litigation, such as terminated employees, longer than other employees. Whenever possible, employees' exit interviews should include questions to ensure that the organization has made a good faith effort to identify and access important operational and legal records, and that the employee will no longer have access to sensitive business information.

In the event of a legal hold, an organization may need to preserve all of a former employee custodian's information to comply with its preservation obligations, as the individual is not available to directly manage the information in compliance with the preservation notice. This can lead to significant over-retention, especially in organizations with large litigation portfolios, where one legal hold can overlap with the next.

D. Shared File Sites

Shared file areas such as network departmental folders or SharePoint often become unwieldy when there is no software available or configured to connect information to retention schedule categories.

---

[70] In *Phoenix Four, Inc. v. Strategic Res. Corp.*, the court, though declining to issue an adverse inference, determined that the elements of an adverse inference instruction were satisfied when unproduced information was found on the dissolved organization-defendant's server during a routine repair call. The court made this determination despite the defendant's explanation that the ignorance of the existence of the information was due in part to the post-dissolution departure of defendant's technical specialist. No. 05-4837, 2006 WL 1409413 (S.D.N.Y. May 23, 2006).

E. Personally Identifiable Information ("PII")

PII may have specific requirements based on privacy laws. Privacy laws may specify how long information must be retained, what and when information must be deleted, and compliant methods of deletion.

F. Law Firms, eDiscovery Vendors, and Adversaries

Outside counsel, legal service providers, and other parties to litigation may also possess copies of an organization's information produced during discovery in legal matters.[71] While counsel have an ethical duty to protect their client's confidences, eventual disposition of client information should be defined by agreement. Depending on the nature of the relationship and the matter, an organization may have different requirements for how long its information should be retained after a matter is closed. Organizations should notify outside counsel of those specific retention requirements and ensure that counsel are able to, and at the appropriate time do, comply with the requirement to dispose of such information. Work-product and attorney-client communications are distinct from preexisting organization business information and may therefore have different retention requirements.

As part of litigation, an organization may also provide copies of its information to other legal service providers, such as eDiscovery and trial presentation providers, and to other parties in its matters. The organization and its attorneys should consider whether a stipulation, confidentiality agreement, or protective order can help protect the information from further disclosure and ensure its proper disposition at the end of the case. For example, the organization may want to limit access to its information to the adversary's outside counsel and their consultants and experts, but bar access by in-house counsel. Or, if in-house counsel does gain access to the documents, at least limit access to prevent other individuals in the organization who do not need access to this information from seeing the information. Also, a protective order might reasonably require that all persons who get copies of the information, including counsel, experts, and anyone else, be required to certify at the end of the case that all copies of the information in question have been returned to the organization or destroyed. Still, other provisions may prohibit the use of the information in any other litigation, or its production to other parties in discovery—at least without notice to the producing party. Provisions such as these may be the organization's best chance to make sure its business information does not fall into the hands of competitors or other adversaries after litigation.

G. In-House Legal Departments

In-house legal departments may suffer similar problems as outside counsel, as described above, because they often receive copies of information from elsewhere in the organization. Robust tracking and classification systems are key to addressing this issue.

---

[71] For an in-depth discussion of information security, privacy, and retention considerations for third-party legal service providers, *see* The Sedona Conference, *Commentary on Privacy and Information Security: Principles and Guidelines for Lawyers, Law Firms, and Other Legal Service Providers*, 17 SEDONA CONF. J. 1 (2016).

H. Hoarders

Audits should be conducted regularly to identify users who are in violation of the Information Governance program. This could include users who routinely back up email to their computer, use an external storage device (best to forbid this outside of special permission), or use shared network storage to save stale content. Ideally, an organization's information disposition system will identify content by date last modified, date last accessed, date created, and file type; each of these metadata fields may be used to monitor for potential violators of the Information Governance program.

I. Regulations

Organizations should make certain that their information management processes and Information Governance policies and procedures consider all applicable regulations including "approved but not yet adopted" regulations (e.g., The General Data Protection Regulation, which was adopted in April 2016 but had a May 25, 2018, enforcement date) as appropriate.

J. Cultural Change and Training

An organization should clearly outline its expectations for compliance with each component of the information lifecycle, including disposition. Disposition of data in particular can be met with resistance by employees who fear they will lose valuable information. Successful program implementation depends on the organization's ability to change employees' existing behavior, which is best achieved when the organization communicates its new expectations in an efficient manner to employees and provides adequate education and training on new policies and procedures.[72] A successful Information Governance program must have support from the organization's senior management with regard to funding and a commitment to cultural change.

---

[72] For example, implementing an automated records management program should incorporate procedures whereby personnel can designate discrete data for preservation for legal or other organizationally defined reasons. Personnel should be aware of and trained on how to efficiently use these systems.