EDDE JOURNAL

A Publication of the E-Discovery and Digital Evidence Committee
ABA Section of Science & Technology Law

SUMMER 2012 VOLUME 3 ISSUE 3

Standards & Guidelines Used to Support the Generally Accepted Recordkeeping Principles

By John Isaza

In the last issue of the *EDDE Journal,* John Isaza introduced the Generally Accepted Recordkeeping Principles (GARP®) for use in developing legally defensible records and information management (RIM) programs. In that article, Mr. Isaza noted how GARP® is "the culmination and amalgamation of years of best practices and various industry standards." In this second article, Ms. Helen Streck, the CEO of Kaizen InfoSource LLC has generously agreed to share a detailed list of RIM standards and guidelines she has collected over the years…. most of the standards and guidelines were considered to arrive at the GARP® principles. *Read more*

Document Hoarding Redux: Law Firms, Don't Fall Prey to the Risks of Electronic Data Over-Preservation

By Anne Kershaw and Shannon Spangler

Picture this: You are the risk management partner for an AmLaw 200 firm. Sheila, leader of your litigation team and a seasoned trial lawyer, interrupts your desk-top lunch to get your perspective. A year ago, she won a defense verdict in federal court for a corporate client. After the verdict, the case settled quickly for waiver of costs. Thereafter, because the company and Sheila reasonably believed this was a one-off case, your firm advised the client that it could dissolve the legal hold and manage its documents and data pursuant to its usual retention policies. The client – very buttoned up with respect to electronic data management -- appropriately disposed of many of the electronic documents that were produced *Read more*

E-Discovery's New Frontier: What the Increase in Portable Corporate Communication Means for E-Discovery

By Skye L. Perryman, Alexander B. Hastings, and Edward H. Rippey

Portable Electronic Devices (PEDs) -- such as BlackBerrys, iPads, and smart phones -- are crucial in modern business communication. It is now common corporate communications to occur via these devices, as opposed to face to face meetings or e-mails from desktop computers. The proliferation of PEDs raises several issues for the preservation and collection of electronic data in litigation and investigations required under the Federal Rules of Civil Procedure and state equivalents. Ensuring best practices relating to information stored on PEDs will become even more critical as the use of such devices expands. *Read more*

Five Proportionality Principles That Can Reduce eDiscovery Costs and Burdens

By Philip Favro

Talk to most any enterprise about legal issues and invariably the subject of eDiscovery will come up as a thorny pain point. These discussions typically focus on the high costs of eDiscovery, particularly for data preservation and document review. Such costs and the inevitable delays that accompany the discovery process provide ample justification for organizations to be on the alert for ways to address these issues. As a solution to these costs and delays, the eDiscovery cognoscenti are emphasizing the concept of "proportionality." *Read more*

Standards & Guidelines Used to Support the Generally Accepted Recordkeeping Principles®

By John Isaza

In the last issue of the EDDE Journal*, John Isaza introduced the Generally Accepted Recordkeeping Principles (commonly known as GARP®) for use in developing legally defensible records and information management (RIM) programs. In that article, Mr. Isaza noted how GARP® is "the culmination and amalgamation of years of best practices and various industry standards." In this second article, Ms. Helen Streck, the CEO of Kaizen InfoSource, LLC has generously agreed to share a detailed list of RIM standards and guidelines she has collected over the years.* Although Ms. Streck admits that she has not updated the list in the last couple of years, *most of the standards and guidelines cited in her compilation were considered to arrive at the GARP® principles*, published in the fall of 2009. For the readers of this article, this is surely a valuable legal tool. If for some reason a court or a party opponent is not convinced that the GARP® principles apply, then the actual standards cited here may serve as the uncontroverted source.

To recap the point of Mr. Isaza's article, by following comprehensive compliance guidelines, including the retention and disposition requirements imposed by GARP® or the following compilation of standards and guidelines, organizations have the tools to manage data that could be used to defend their RIM policies in court. These standards must be applied to all sources of information within the organization to ensure good faith business practices that are defensible in court and before auditing agencies. Furthermore, since RIM essentially sits at the cusp of eDiscovery efforts, if it is managed properly and in accordance with robust and enforced policies and procedures, organizations should be able to reduce the volume of information available for preservation, collection, analysis and production in litigation.

The list has the following columns:

- Source
- Legal Principle / Professional Standard (Text provided where available; summary provided otherwise)
- Control Objective
- Procedures
- Other Related Industry Guidance (this is shown where applicable under the description of the principle / standard)

Source	Legal Principle / Prof Standard	Control Objective	Procedures
The Sedona Guidelines, Second Edition: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age (The Sedona Conference® Working Group Series, 2007) **[hereinafter The Sedona Guidelines]**, Guideline 1, Comment 1.b.	"An organization should have reasonable policies and procedures for managing its information and records."	To achieve efficiency and legal/administrative defensibility of enterprise records management	An Information and Records Management[1] Policy shall be approved by management, published and communicated to all employees.
Other Related Industry Guidance: The U.S. Supreme Court noted that a reasonable records and information management policy should be considered in determining appropriate consequences for the destruction of evidence. The Sedona Principles, Second Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production (The Sedona Conference® Working Group Series, 2007) **[hereinafter The Sedona Principles]**. Comment 1.b.; see also, The Sedona Principles, Comment 5.b.			
The Sedona Guidelines, Guideline 2.	"An organization's information and records management policies and procedures should be realistic, practical and tailored to the circumstances of the organization."	To develop an enterprise records management system that is reasonable under all the circumstances, considering available guidance and the unique circumstances of the organization	
The Sedona Guidelines, Comment 2.b.	"Information and records management requires practical, flexible and scalable solutions that address the differences in an organization's business needs, operations, IT infrastructure and regulatory and legal responsibilities."	To assure that Information and Records Management Programs are flexible, practical and scalable	The Corporation should develop processes and procedures that meet the business and legal requirements.
The Sedona Guidelines, Comment 2.c.	"An organization must assess its legal requirements for retention and destruction in developing an information and records management policy."	To prevent destruction of records that might lack business value but are otherwise subject to legal and regulatory preservation requirements	The Corporation should create a records retention schedule and procedures for implementing the retention schedule for complying with legal retention requirements.

Other Related Industry Guidance: Courts have held that parties responding to litigation discovery are best situated to evaluate the procedures, methodologies, and technologies appropriate for preserving and producing their own electronically stored information. See The Sedona Principles, Principle 6, with Comments and cases cited therein.			
The Sedona Guidelines, Comment 2.d.	"An organization should assess the operational and strategic value of its information and records in developing an information and records management program."	To prevent over-retention of information that lacks value and is not otherwise subject to preservation	The Corporation should conduct and assessment of the value of its information in developing policy and procedures.
The Sedona Guidelines, Comment 2.e; The Sedona Principles, Comment 5.h.	A business continuation or disaster recovery plan has different purposes from those of an information and records management program. The two should be separated where such separation will benefit the organization.	To separate active data and archival data from data required only for disaster recovery	The Corporation shall clearly establish distinct standards and procedures for both archiving and disaster recovery backup processes.
Other Related Industry Guidance: Neither disaster recovery backup tapes, nor shadowed, fragmented, or residual data are primary sources of litigation discovery. See The Sedona Principles, Principles 8 and 9. It follows that appropriate management--including the complete destruction of such data that has no business value and is not subject to a preservation obligation--may further help prevent expensive litigation discovery disputes and mitigate the unnecessary costs of over-retention.			
The Sedona Guidelines, Guideline 3.	"An organization need not retain all electronic information ever generated or received."	To prevent over-retention of information and to ensure it is reasonably destroyed in good faith	

The Sedona Guidelines, Comment 3.a.	"Destruction is an acceptable stage in the information life cycle; an organization may destroy or delete electronic information when there is no continuing value or need to retain it."	To prevent over-retention of information that has become obsolete and not subject to preservation	Proven systematic deletion and/or destruction of obsolete information, records, and metadata is conducted regularly.
The Sedona Guidelines. Comment 3.c.	"Absent a legal requirement to the contrary, organizations may adopt programs that routinely delete certain recorded communications, such as electronic mail, instant messaging, text messaging and voicemail."	To prevent retention of messages that do not qualify as records for retention under the applicable policy	The Corporation shall define the appropriate criteria for determining which type of electronic messages shall be retained.
The Sedona Guidelines, Comment 3.d.	"Absent a legal requirement to the contrary, organizations may recycle or destroy hardware or media that contain data retained for business continuation or disaster recovery purposes."	To prevent retention of obsolete hardware or media for which retention is not required under the applicable policies	The Corporation shall document and follow a systematic approach for the recycle and reuse of disaster recovery backup tape.
The Sedona Guidelines, Comment 3.e.	"Absent a legal requirement to the contrary, organizations may systematically delete or destroy residual, shadowed or deleted data."	To prevent the burdens and costs associated with the retention of residual, shadowed or deleted data when there is no retention requirement for the original and complete copy	The Corporation may document and follow a systematic approach to overwrite and delete forever residual, shadowed or deleted data.
The Sedona Guidelines, Comment 3.f.	"Absent a legal requirement to the contrary, organizations are not required to preserve metadata; but may find it useful to do so in some instances."	To prevent costly data mining and data storage where there is no retention requirement for metadata	The Corporation may create a procedure for systematically deleting metadata that is obsolete.
Other Related Industry Guidance: AIIM TR31/4: 1994 (R1999)			

The Sedona Guidelines, Guideline 4	"An organization adopting an information and records management policy should also develop procedures that address the creation, identification, retention, retrieval and ultimate disposition or destruction of information and records."	To provide the appropriate governance and controls that manage records and information throughout its lifecycle	The Corporation shall develop procedures to manage the lifecycle of records and information as the part of normal governance process.
The Sedona Guidelines, Comment 4.a.	"Information and records management policies must be put into practice."	To achieve intended results in managing records and information	Policies and procedures must be regularly implemented.
The Sedona Guidelines, Comment 4.b.	"Information and records management policies and practices should be documented."	To monitor compliance and provide defensibility	The Corporation shall ensure that procedures are documented and available.
The Sedona Guidelines, Comment 4.c.	"An organization should define roles and responsibilities for program direction and administration within its information and records management policies."	To create accountability and prevent overlap	Roles and responsibilities are defined and documented in accordance with the Policy.
The Sedona Guidelines, Comment 4.d.	"An organization should guide employees regarding how to identify and maintain information that has a business purpose or is required to be maintained by law or regulation."	To facilitate compliance with records policies	The Corporation shall provide classification schemes and boundaries for organizing and indexing information.
The Sedona Guidelines, Comment 4.f.	"An organization should consider the impact of technology on the creation, retention and destruction of information and records."	To determine efficiencies and potential liabilities	The Corporation should conduct and document a business impact analysis of the use of technology for managing information and records.
The Sedona Guidelines, Comment 4.g.	"An organization should recognize the importance of employee education concerning its information and records management program, policies, and procedures."	To facilitate compliance with records policies	The Corporation should develop an education and training course to define the IRM Program Policy requirements.

The Sedona Guidelines, Comment 4.h.	"An organization should consider conducting periodic compliance reviews of its information and records management policies and procedures, and responding to the findings of those reviews as appropriate."	To document compliance for defensibility, to ensure preservation of vital business information, and to timely correct errors	The Corporation should conduct regular compliance reviews of its information, document the findings of these reviews and develop a corrective action plan.
The Sedona Guidelines, Comment 4.i.	"Policies and procedures regarding electronic management and retention should be coordinated and/or integrated with the organization's policies regarding the use of property and information, including applicable privacy rights or obligations."	To create a comprehensive records management scheme	The Corporation should ensure that IRM policies and procedures are coordinated with other governance documents to protect the organizations property, information and privacy rights or obligations.
The Sedona Guidelines, Comment 4.j.	"Policies and procedures should be revised as necessary in response to changes in workforce or organizational structure, business practices, legal or regulatory requirements and technology."	To ensure the maintenance of effective and efficient policies and compliance with laws and regulations	Policies and procedures should be revised as necessary in response to changes in business practices, legal or regulatory requirements or technology.
The Sedona Guidelines, Guideline 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."	To comply with litigation, government investigation, or audit preservation obligations	Procedures should be developed to determine when it is appropriate to suspend normal practices
The Sedona Guidelines, Comment 5.a.	"An organization must recognize that suspending normal destruction of electronic information and records may be necessary in certain circumstances."		Procedures should be developed to document the process for suspending the normal practice and identify the individuals with the responsibility to implement, distribute and publish legal holds.

The Sedona Guidelines, Comment 5.b.	"An organization's information and records management program should anticipate circumstances that will trigger the suspension of normal destruction procedures."		The IRM Program should have a documented process for efficiently and effectively communicating legal holds to affected individuals.
The Sedona Guidelines, Comment 5.d.	"An organization's information and records management procedures should recognize and may describe the process for suspending normal records and information destruction and identify the individuals responsible for implementing a legal hold."		The Corporation should include in their procedures a mechanism to suspend normal retention practices. The issuance of a "Legal Hold" under direction of the Law Department must suspend normal information and records retention schedules and identify the individuals that may have relevant information.
Other Related Industry Guidance: Courts have held that the duty to preserve evidence for litigation that should be reasonably anticipated transcends records management policies, but the scope of the preservation duty is not boundless and is subject to reason. See The Sedona Principles, Principles 1 and 5, with Comments and cases cited therein.			
The Sedona Guidelines, Comment 5.f	"Effectively communicating notice of a legal hold should be an essential component of an organization's information and records management program."	To facilitate compliance with the legal hold	Procedures should be developed to ensure employees receive and appreciate the import of a "Legal Hold."
Other Related Industry Guidance: Failure to initiate reasonable preservation protocols as soon as practicable may increase the risk of disputes that relevant information was not preserved. The Sedona Principles, Comment 5.c.			
The Sedona Guidelines, Comment 5.i	"Legal holds are exceptions to ordinary retention practices and when the exigency underlying the hold no longer exists, organizations are free to lift the legal hold."	To prevent over-retention when preservation obligations have abated	The IRM Programs should develop a process for communicating the change back to the normal practice once the legal hold has been lifted.

ANSI/ARMA; Society of American Archivists; Sedona Conference Glossary ANSI/ARMA 10-1999 Glossary of Records and Information Terms (3rd Edition)	Industry organizations have established a standardized lexicon for a RIM Program.	To standardize the terminology used for the RIM Program	The Corporation should develop and publish a standardized RIM Glossary of Terms.
ANSI/ARMA; NFPA; NFPA;ANSI/ARMA TR-01-2002 ARMA: Records Center Operations: Section 1.2 NFPA 13 NFPA 232: Section 1.1.	Industry standards provide requirements for records protection equipment and facilities and records-handling techniques that provide protection of records in a variety of media forms from hazards of fire.	To ensure the safety and protection of records and information	The Corporation should develop a set of criteria by which to evaluate or operate an offsite storage facilities for storing records and information.
Other Related Industry Guidance: NARA Guidance			
ANSI/ARMA 8-2005: Retention Management for Records and Information Management: Section 7.0 - Developing the Information Retention and Disposition Program; Section 8.0 Review and Approval	Establish and operate an information retention and disposition program as a component of a complete Records and Information Management (RIM) program.	To define an established process for developing and approving a records retention schedule.	The Corporation should develop a Records Retention Schedule that defines the retention requirements for records and information.
ANSI/ARMA 8-2005: Retention Management for Records and Information	This standard covers general principles in structuring an information retention and disposition program including authority and responsibility.	To create a comprehensive defensible process for information disposition.	
Section 1.2	Organizations should include a retention and disposition program as a component of a RIM Program.	To establish the processes for the appropriate disposition of information and avoid unnecessary retention of obsolete information	The Corporation should develop regular processes that are designed to retain information only for as long as there is business value or legal requirements.

Section 10	"Disposition of records should be completed in the normal course of business an incompliance with approved retention periods and established procedures."	To ensure effective and efficient access to records and information as needed	Develop the appropriate procedures and controls for the final disposition of records and information.
ANSI/ARMA 12-2005: Establishing Alphabetic, Numeric and Subject Filing Systems	"Standardization of filing systems ensures that all records, regardless of media, are properly and consistently housed, identified, and maintained so that they may be efficiently and effectively retrieved using standard equipment, practices and procedures."	To facilitate access to records and information on an ongoing basis	Develop a taxonomy or classification that provides the appropriate structure for indexing records and information.
Other Related Industry Guidance: AIIM TR40-1995 NISO TR02-1997 NISO TR03-1999			
Records Management Responsibility in Litigation Support:	Industry guidance is to assist records managers in defining their roles in the litigation process.	To define and establish the role and support of the RIM Program in a litigation proceeding	The Corporation should define the role of records and information in the eDiscovery process.
ANSI/ARMA 9-2004: Section 1.1 Requirements for Managing Electronic Messages as Records	This standard provides instruction on how to formulate an electronic messaging policy representative of an organization's unique environment.	To establish the criteria for defining emails that are records and for the appropriate management of those records	The Corporation should establish standardized criteria to define when electronic messages are to be categorized and managed as records.
ARMA/ANSI Standard 5-2003: Section 1.2	This standard provides guidance for identifying those organizational records and information that are deemed vital and provides standards for methods of protecting them.	To protect the records and information vital to the operation, legal and financial position of the organization	The Corporation should develop procedures and controls for managing and protecting the vital records.
Other Related Industry Guidance: NARA Guidance			

ISO 15489-1: Section 6.1 and ISO/TR 15489-2 Information and DocumentationIncluding ISO 9001 and ISO 14001	The standard recommends that organizations establish, document, maintain and promulgate policies, procedures, and practices for records management to ensure that its business need for evidence, accountability and information about its activities is met.	To document the requirements for managing records and information that are evidence of the business activity of the organization	The Corporation should developed, adopted and endorsed a RIM policy at the highest decision-making level.
ISO 15489-1: Section 6.3 and ISO/TR 15489-2 Information and Documentation Including ISO 9001 and ISO 14001	Records management responsibilities and authorities should be defined and assigned, and promulgated throughout the organization.	To assign authority and accountability for the RIM Program and define employee expectations	Ownership and accountability for the RM Program should be assigned. Create job descriptions and developmental plans for all employees who fulfill a role in the RM Program.
ISO 15489-1: Section 7.1 and ISO/TR 15489-2 Information and Documentation Including ISO 9001 and ISO 14001	Organizations should create and maintain authentic, reliable and useable records, and protect the integrity of those records for as long as required.	To maintain the integrity and reliability of records for future use	Develop a comprehensive program to include: a. determine what records should be created b. decide what form and structures of records and the technologies used c. determine what metadata to capture d. determine access requirements e. decide how to organize for use f. preserve records and make available over time g. comply with legal/regulatory requirements h. ensure records are safe and secure i. ensure records are retained only as long as necessary
ISO 15489-1: Section 8.2.2 and ISO/TR 15489-2 Information and Documentation Including ISO 9001 and ISO 14001	Any system deployed to manage records should be capable of continuous and regular operation in accordance with responsible procedures.	To ensure the ongoing access to records and information	Procedures should be established that document the normal business process for managing records.

ISO 15489-1 Section 8.3.6 and ISO/TR 15489-2 Information and Documentation Including ISO 9001 and ISO 14001	Provide timely and efficient access to, and retrieval of, records needed in the continuing conduct of business and to satisfy related accountability requirements.	To ensure reliability and support ongoing access for future business use	Records systems should have accurately documented procedures and processes that provide for access and use of records and information.
ISO 15489-1 Section 8.3.2 and ISO/TR 15489-2 Information and Documentation Including ISO 9001 and ISO 14001	Records systems should contain complete and accurate representations of all transactions that occur in relation to a particular record.	To provide the integrity of the organization's records and information	The Company should develop a set of RIM criteria and features that will be required in the design of an Electronic Records Management application.
ISO 15489-1 Section 8.3.3 and ISO/TR 15489-2 Information and Documentation Including ISO 9001 and ISO 14001	Appropriate storage environment and media, physical protective materials, handling procedures and storage systems should be considered.	To protect and safeguard records and information for future access and use	The Corporation should develop a set of criteria by which to evaluate offsite storage facilities for storing records and information.
Other Related Industry Guidance: ARMA Guidelines NARA Guidance NFPA 13 NFPA 232			
ISO 15489-1 Section 8.2.4 and ISO/TR 15489-2 Information and Documentation Including ISO 9001 and ISO 14001	Records systems should be managed in compliance with all requirements arising from current business, the regulatory environment and community expectations in which the organization operates.	To document and demonstrate compliance	The Corporation should develop audit criteria for evaluating the effectiveness of the RIM Program and reporting the results to management.
ISO 15489-1: Section 8.2.6 and ISO/TR 15489-2 Information and Documentation Including ISO 9001 and ISO 14001	Records should be created, maintained and managed systematically.	To demonstrate repetition as evidence of compliance	Procedures should be established that routinely document the normal business process for managing records.

ISO 15489-1 Section 8.3.4 and ISO/TR 15489-2 Information and Documentation Including ISO 9001 and ISO 14001	Records systems should be capable of supporting alternative options for the location of records.	To facilitate effective and efficient access to records and information	Storage media and environments should be designed to ensure the availability and accessibility of records as long as they are required to exist.
ISO 15489-1 Section 8.3.5 and ISO/TR 15489-2 Information and Documentation Including ISO 9001 and ISO 14001	Records systems should be designed so that records will remain authentic, reliable and useable throughout any kind of system change.	To demonstrate the integrity of records and information regardless of system or media change	Develop a plan and established criteria and procedures for transferring data during system changes or system decommissioning.
ISO 15489-1 Section 8.3.6 and ISO/TR 15489-2 Information and Documentation Including ISO 9001 and ISO 14001	Records systems should provide timely and efficient access to, and retrieval of, records needed in the continuing conduct of business and to satisfy related accountability requirements.	To ensure that records and information are available, findable and accessible when needed	Develop procedures and criteria for classifying, indexing and tracking records and information.
ISO 15489-1 Section 8.3.7 and ISO/TR 15489-2 Information and Documentation Including ISO 9001 and ISO 14001	Records systems should be capable of facilitating and implementing decisions for the retention or disposition of records.	To ensure that obsolete records and information are appropriately disposed	The Corporation should develop system requirements or protocols for implementing the requirements of the Records Retention Schedule.
ISO 15489-1 Section 9.6 and ISO/TR 15489-2 Information and Documentation Including ISO 9001 and ISO 14001	Records should be stored on media that ensures their usability, reliability, authenticity and preservation for as long as they are needed.	To ensure the integrity and accessibility of records and information	Develop procedures for converting or migrating records from one records system to another. Develop standardized criteria to be used in evaluating, selecting and using media to ensure the availability and accessibility of records as long as they are required to exist.
ISO 15489-1 Sections 9.8.2 and 9.8.3 and ISO/TR 15489-2 Information and	A records system should be able to track the movement and use of records within the system.	To identify actions needed, enable retrieval, prevent loss, monitor usage, and maintain capacity	Develop procedures for allocating and tracking the decisions or transactions of a record.

Documentation Including ISO 9001 and ISO 14001			Develop a mechanism and associated procedures for tracking the location of records.
Other Related Industry Guidance: ANSI/AIIM/ARMA TR48-2006			
ISO 15489-1 Section 9.9 and ISO/TR 15489-2 Information and Documentation Including ISO 9001 and ISO 14001	Disposition authorities that govern the removal of records from operational systems should be applied to records on a systematic and routine basis.	To demonstrate routine compliance that obsolete records and information are appropriately disposed	Develop requirements or protocols within a RIM system for implementing the requirements of the Records Retention Schedule.
ISO 15489-1 Section 9.10 and ISO/TR 15489-2 Information and Documentation Including ISO 9001 and ISO 14001	Documentation describing records management processes and records systems should address legal, organizational and technical requirements.	To demonstrate through documentation compliance with legal, regulatory and technical requirements	The Corporation should have the RIM strategy and policy requirements reviewed by the appropriate groups and levels.
ISO 15489-1 Section 10 and ISO/TR 15489-2 Information and Documentation Including ISO 9001 and ISO 14001	Compliance monitoring should be regularly undertaken to ensure that the records systems procedures and processes are being implemented according to the organizational policies and requirements.	To ensure routine compliance with legal, regulatory and technical requirements and to identify gaps in program processes and controls	The Corporation should develop an auditing process to measure compliance and a mechanism for corrective action.
ISO 15489-1 Section 11 and ISO/TR 15489-2 Information and Documentation Including ISO 9001 and ISO 14001	Organizations should establish an ongoing program of records training.	To assure employees understand and compliance with program requirements and expectations	The Corporation should develop a RIM education and training strategy and the courses to support this strategy.
ISO 23081-1 Metadata for Records - Part 1 (aligns with ISO 14589 requirements).	System and business requirements for metadata classification should include capture/store/use criteria of records and information.	To provide an audit trail of actions on records and information	The Corporation should develop the criteria it wants in defining metadata that will be created and captured.

ISO 19005: PDF/A - Archival of PDF Documents	The standard defines the criteria for archiving electronic documents that are already in PDF format.	To develop long-term preservation of historical electronic information	The Corporation should include the requirements of this standard within their electronic records and information archiving strategy.
ANSI/NISO Z39.48-1992 (R2002) Section 1.1. Purpose	Establishes criteria for coated and uncoated paper that will last several hundred years without significant deterioration under normal use and storage conditions.	To preserve historical records in paper format	The Corporation should include the requirements of this standard within historical paper records preservation protocols.
U.S. Department of Defense 5015.2: Design Criteria Standard for Electronic Records Management Software Applications	Sets forth the minimum baseline functional requirements, and identifies non-mandatory features deemed desirable for an Electronic Records Management Software Application.	To develop a set of RIM criteria and features that will be required and suggested in the design of an Electronic Records Management application.	The Company should develop a set of RIM criteria and features that will be required in the design of an Electronic Records Management application.
ARMA Standards Development Program Projects - In Progress[2]	Electronic Records Management Software Application: Design Criteria	1. Provide procedural- and implementation-related information on the management of electronic records. 2. Inform of the utility of the DoD standard, identifying those requirements which are usually considered to be relevant to the commercial/private sector and those that are not. 3. Describe how to take advantage of features provided in a DoD-certified RMA, including those features thought to be non-relevant. 4. Indentify gaps in DoD requirements of RIM functions.	Not out yet

	Guideline on Contracted Destruction for Records and Information Media.	1. Provide a list of destruction methods in support of NIST Guidelines. 2. Provide a list of recommended destruction methods. 3. Address vendor selection criteria based on the recommended destruction methods - NAID Vendor Selection Guidelines. 4. Provide quality control guidelines - Auditing Vendors (NAID Guidelines) 5. Provide Case Law and Legal Requirements.	Not out yet
	Metadata	Provide information in an educational format that can be utilized in diverse industry setting. Topics include: Definition/importance of metadata Classification/indexing/taxonomy Recommendations for use of metadata Role of metadata within diverse functional/professional areas.	Not out yet
	Records and Information Management for Information Technology Professionals	The guideline will examine the relationship between RIM and IT, indicating how the two work together. Topics include: IT and records management overview Information lifecycle Classification and taxonomy Metadata Data migration/legacy systems	Not out yet
	Risk Management	The guideline will describe risks and discuss methodologies that may be applicable within a RIM context: RIM Risks: description of risks, probabilities and impacts and examples of how risk is mitigated Risk Management Methodology: identifying risks; assessing risks; and measuring/monitoring risk	Not out yet

	Website Records Management	Discuss to what extent and under what circumstances information content posted on Internet websites constitutes records. Topics include: Identifying Web records Models and perspectives Processes and assessments Roles and Responsibilities Records retention issues Web capture tools and content management systems	Not out yet
Note: For the purpose of this document Information and Records Management (IRM) and Records and Information Management (RIM) mean the same thing. The choice of the phrase is unique to the standardizing body.			

John Isaza, Esq., FAI (Fellow of ARMA International #45) heads the Information Management practice at Rimon Law Group, PC, a twenty-first century international business law firm. By bringing structure to chaos, John is internationally recognized in the emerging legal field of information governance, as well as records and information management (RIM). He has developed information governance and RIM programs, including related regulatory opinions, for some of the most highly regulated Fortune 100 companies. He has facilitated records retention research in over 130 countries and counting. Prior to joining Rimon, he was the co-founder and Partner of Howett Isaza Law Group, a boutique law firm specializing in corporate compliance matters. John also served as General Counsel to a publicly traded medical device manufacturer, now owned by Abbott Laboratories. He is co-author of 7 Steps for Legal Holds of ESI & Other Documents, and the recipient of ARMA's prestigious Britt Literary Award. Mr. Isaza can be reached at John.Isaza@RIMonLaw.com or 949-715-7010.

Document Hoarding Redux: Law Firms, Don't Fall Prey to the Risks of Electronic Data Over-Preservation

By Anne Kershaw and Shannon Spangler

Picture this: You are the risk management partner for an AmLaw 200 firm. Sheila, leader of your litigation team and a seasoned trial lawyer, interrupts your desk-top lunch to get your perspective. A year ago, she won a defense verdict in federal court for a corporate client. After the verdict, the case settled quickly for waiver of costs. Thereafter, because the company and Sheila reasonably believed this was a one-off case, your firm advised the client that it could dissolve the legal hold and manage its documents and data pursuant to its usual retention policies. The client – very buttoned up with respect to electronic data management -- appropriately disposed of many of the electronic documents that were produced in the first case in compliance with its normal retention policies.

Three months ago, a different plaintiff filed a nearly identical lawsuit, proving Sheila and her client wrong about the likelihood of repetition. The client issued a new, but nearly identical, legal hold notice for the second lawsuit. Predictably, the plaintiff served the same document requests that were served in the first case. Whew! You thought Sheila was going to lay a real problem at your doorstep. But you know that the advice regarding dissolving the legal hold and returning to normal document retention policies was sound and well documented, and the legal hold for the second case was timely issued. All is well.

But wait -- it turns out that *your firm s*till has copies – multiple – of the very documents that the client disposed of in the ordinary course, post-litigation. After the first lawsuit ended, and the celebrations were over, your litigation colleagues moved on to the next lawsuit, not giving a thought to the firm's file closeout procedures. Sheila's question: must she tell the client about these copies? And must the client produce them in this new lawsuit? After all, as far as the client is concerned, they no longer exist, and there wasn't any obligation to retain them between the first and second lawsuits.

Your chest feels tight. Indigestion? Something more serious?

You take a deep breath and remind Sheila that even though the company (and thus your firm) had no obligation to retain these documents after the first lawsuit ended, the current legal hold obligation trumps the right to dispose. In short, if the documents now exist, they likely must be disclosed if potentially relevant under Fed. R. Civ. P. 26(a), 26(b)(1) and 26(b)(2)(B), and possibly produced under

Fed. R. Civ. P. 34. In addition, lawyers who know of documents preserved for one case that are relevant in another have a duty under Rule 26(g) to disclose the existence of those records.

Now take another deep breath – the client claims that your firm is responsible for all costs and liabilities relating to the improper retention of these documents. Is this claim covered under your firm's professional liability policy? Your carrier will likely argue that these are not covered claims and now you have a coverage dispute in addition to the suit filed by your former client. You may also have violated attorney ethics rules. All this, because no one took the time to properly and completely close the matter and throw out the documents. This article provides workable and cost-effective recommendations that will keep this scenario from happening to you.

Many recent articles[1] address businesses' habit of data hoarding – routinely storing vast amounts of electronic data (and perhaps paper) they are neither required to keep by law nor have a business need to save. Business executives and their lawyers worry that the data contains information that *might* be subject to a legal hold and *might* be relevant to some existing or as yet unknown future litigation – and the destruction of this data *might* be second-guessed by adversaries and courts. So it is not surprising that so many are reluctant to say "throw it out" and risk spoliation sanctions, even if that risk is remote. Yet saving everything to avoid sanctions is not an insurance policy; to the contrary, it actually increases risk. For law firms, which are as likely to fall victim to the same conclusions about their data, there are additional risks that may arise from retaining client data unnecessarily.

In corporations, we find that 80% of ostensibly "active" files and folders on hard drives and in file shares have not been accessed for 3 to 5 years. In other words, 80% of the electronic files are essentially dead – yet IT spends money on these dead data daily for infrastructure, disaster recovery, and data migration as old servers and systems are retired. Some organizations also pay to store tens of thousands of backup tapes, all essentially useless. Other costs are hidden, much like coronary artery disease - such as lost attorney and paralegal time spent wading through unused and unwanted information to find what they need or lost informational value of content management systems because there is simply too much clutter.

Law firms are not immune from similar over-saving of data having little-to-no future value. Law firms, rightfully reluctant to invest in unnecessary infrastructure, will recognize the business case for properly

[1] *See, e.g.,* Anne Kershaw, See What Lurks Within: Destroy legacy data or it can come back to haunt your company, by Anne Kershaw, Law Technology News, December 1, 2011 <http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202533293136> [visited April 22, 2012]; John Chapras II, Auld Lange Syne New Year's Resolution: In 2012, keep the gold and discard the dangerous, Law Technology News, December 1, 2011 http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202533293946 [visited April 22, 2012]; Survey Finds Infinite Data Retention Leading to Costly Information Management Mistakes, August 4, 2010 <http://www.symantec.com/about/news/release/article.jsp?prid=20100804_01> [visited April 22, 2012]; Matthew Minor, "Alignment of Document Retention and Litigation Hold Strategies Is Key to Defensible Data Deletion," February 13, 2012 <http://www.ezinearticles.com/?Alignment-of-Document-Retention-and-Litigation-Hold-Strategies-is-Key-to-Defensible-Data-Deletion&id=6864559> [visited April 22, 2012].

managing their own data, as well as the obvious operational costs associated with data hoarding; it costs money to maintain, backup and expand electronic data storage. While these operational costs can be significant, we know that the most visible costs associated with data hoarding can be legal expenses. No law firm wants to incur unnecessary expense when it faces its own litigation issues. Document review is often the largest single expense in litigation and can quickly mount to hundreds of thousands of dollars, if not millions. When it comes to a law firm's administrative data – such as law firm financial records and employee files – the risks of over saving likely are indistinguishable from those that any business might embrace by keeping unneeded data. Law firms will face the same "just in case" resistance to disposing of documents that any other organization does, and the lawyers and other staff will balk at the time commitment involved in thoughtful disposition.

In addition, special problems arise for law firms holding client information and documents, transmitted to or created by the law firm in connection with the representation. These could be company business documents provided for purposes of conducting an investigation, for fact development in litigation, or for review and production in discovery. Some documents may be privileged, others may contain confidential business or trade secret information, and still others may include privacy information.[2] The documents and data provided to the law firm are likely to be copies, but it is possible for law firms to either hold or create unique client documents (for example, through addition of notations) – and unless appropriate controls were in place when the law firm received and handled the documents, it is also possible that no one will know which is which after the fact. Law firm case files also may contain documents generated for the client that "belong" to the client under applicable state law.[3] No attorney would *intentionally* create significant eDiscovery issues for a client (and possibly liability issues for the firm), but law firms may end up in the same place through *inattention* -- by failing to implement and follow case file closing and records management procedures. In short, law firms should dispose of data when it is eligible for disposition, before a matter arises, thus minimizing the risk of incurring these potential costs and liabilities.

---

[2] Retaining data unnecessarily can also contribute to the risk of loss or disclosure of privacy data. Organizations are increasingly feeling the sting of state privacy legislation that requires notification of state officials and implicated state citizens if the private information pertaining to their citizens, such as social security numbers or credit card numbers, is breached or disclosed. Damages in individual incidents involving the actual loss of credit card information have exceeded a hundred million dollars, e.g. Google "TJX credit card breach" or "Heartland payments systems breach costs." In addition, class actions are being filed against organizations for privacy breaches. *See* John F. Mullen and Francis X. Nolan IV, "Future of Data Breach Class Actions After 'Anderson'", April 12, 2012 <http://www.newyorklawjournal.com/PubArticleNY.jsp?id=1202548660451&Future_of_Data_Breach_Class_Actions_After_Anderson&slreturn=1> [visited April 22, 2012]. Law firm data breaches happen as well. The best protection against a privacy breach is to dispose of the data as soon as it is no longer needed. Hackers and thieves can't take what you don't have.

[3] State law treatment of the question of client ownership of law firm file materials is not uniform. Generally, clients are treated either as (1) owning some portion of the file, including documents it provided to the lawyers, original documents with independent legal significance, and final work product or (2) having some right of access to these and perhaps other file materials. *See, e.g.,* Julie J. Colgan, *The Ethical Custodian – aka The Messy Truth About Records & Information Management in Law Firms,* <http://www.e-legaltechnology.org/member-articles/article-detail.php?id=18> [visited April 22, 2012]. The ABA Model Rules of Ethics provide only bare-bones guidance in Rules 1.16(d) and 1.15.

Some questions to consider in evaluating your data hoarding quotient:

- Do you know what client data you have and where it is stored? Are client and firm data commingled, for example, on disaster recovery systems? Do other third parties, such as processing and hosting vendors, experts, and opposing counsel, hold the client's data in connection with the representation?
- Do you "decide" to retain documents through sheer post-litigation inattention, thus depriving the client of rights it may have with respect to this data and failing to counsel the client regarding electronic data risks? What roles do you and the client play in determining whether data should continue to be retained once a legal hold obligation has expired?
- Do you routinely counsel clients in both the technological and legal aspects of electronic data and eDiscovery, and do you have experience making disposal recommendations with respect to legacy data? Do you have appropriate professional liability coverage for such recommendations?

To avoid a law firm coronary event like the one described above, there are two possible approaches. One is to advise all partners in the firm of the risks associated with retaining data they should not keep, that these liabilities are likely not covered by insurance, and further advising that they will be held personally liable for any claims. We believe that the better approach, however, is for the law firm to employ a series of processes to evaluate its data retention practices and dispose of both administrative and client data that are not legally required to be held and serve no ongoing business purpose. In other words, launch a workable and cost-effective electronic data housecleaning program, as follows.

First, review the firm's records retention and legal hold policies and evaluate how they apply to both its own administrative data and any client records it may have in its files. Do the policies specifically cover electronic information? Do they address client data and prescribe post-litigation and/or post-representation document management procedures, including protocols to properly dispose of data in the hands of the law firm and other third-party vendors? Is the management of client data addressed in engagement letters, and are those provisions regularly followed?

Next, map the firm's data systems and inventory its data. Where is active firm data held? -- Probably in numerous places, including file shares and email folders. In addition, the firm should identify its legacy data sources, such as hard drives, servers, archives and/or back-up disaster recovery tapes. The firm should extend this inventory process to include any client data it holds. And, don't forget those third-party vendors and opposing counsel: into what other hands has the firm (or the client) put client data? This step is often best completed by simply issuing a survey within the firm.

Once the firm has a good grip on what it has where, it should identify, by folder or container, data that is transitory and eligible for deletion versus data that is subject to a records retention schedule or

otherwise must be held for legal reasons or in connection with an active client matter. This involves different processes for different types of data but, overall, should not be done on a document by document level. Rather, decisions must be made on a higher level. For example, folders in file shares should be reviewed to determine the dates of last use of the folders and files. Employees are asked to confirm that all scheduled business records are in appropriate repositories and locked down. The search functions now available in operating and email systems can be used to search categories of records that need to be retained. Physical data containers like drives, servers, tapes and other media are inventoried and reasonable efforts made to determine their provenance and whether they are duplicates of data held elsewhere, thus permitting a reasonable evaluation of whether the data is subject to legal hold or may be destroyed.

If the firm's administrative data is required for business, regulatory, or legal hold purposes, it should be placed on retention schedules and catalogued in appropriate databases and repositories so it can be later located. If not, it can – and should be -- disposed of.

If the firm continues to hold client data/documents beyond the expiration of a particular legal hold obligation, the law firm should immediately contact the client and initiate discussion regarding appropriate disposition. Your clients will love you for doing this. Factors that may impact the ultimate decision include the likelihood of like-kind litigation in the future (in which case it may *not* be appropriate to dissolve the hold); whether the data is merely a copy of data held independently by the client; whether the data is inaccessible; and whether the data is commingled with other client or firm data. Of course, the firm and other third-party vendors together may have multiple copies of client data residing in a number of different places, and all copies must be evaluated in the same fashion, although if the decision is to continue to preserve the data, there is rarely a legal or business reason to retain multiple identical copies. One will do.

Finally, the firm must give serious consideration to whether it has the capacity, expertise and risk tolerance to do the housecleaning effort described above. An experienced and properly insured outside consultant or expert, willing to go on record verifying the reasonableness of the firm's processes and recommending the final disposition of records, can bring significant value to the process.[4] Having a legacy data management expert lead the process will also help ensure that the appropriate documentation is created and maintained by the expert and that all applicable privileges are preserved in the event that disposition decisions are later questioned. Data maps, employee

[4] A number of factors will shape the scope of the consultant's engagement, including whether it is appropriate for the consultant to have access to a client's confidential materials. In situations where it is not, the consultant's role may be limited with respect to determining the provenance of data and making specific disposal recommendations. Nonetheless, even where the law firm is not able to eliminate the possibility of conflicts or obtain client approvals for the consultant's access to confidential client data, the consultant can recommend, verify and opine as to the housecleaning *processes* employed, and should also be able to provide substantial assistance in mapping the law firm's systems and identifying where active and legacy data reside. In any event, the law firm must take all proper steps to comply with its obligations to maintain client confidences and follow the clients' instructions regarding the consultant's access to their confidential information.

surveys, inventory lists, memoranda documenting conversations with key IT personnel, firm lawyers and paralegals as well as client representatives regarding the content of various repositories, and notations regarding ultimate dispositions are critical to complete memorialization of the process and results.

In determining whether to use an outside consultant to assist with its electronic data management efforts, the firm should consider first whether it is willing to make the internal investment required to do a meaningful housecleaning. Clients (and certainly former clients) will be reluctant to pay for attorney and paralegal time for case file clean-up long after the fact (and after case budgets may have been closed). It may not be possible to pull resources away from other client/case needs to do a project of this magnitude, or, more simply, it may not make economic sense.

Second, does the law firm have the requisite expertise? Judges and academics speak more and more often about the question of eDiscovery competency. *See, e.g.,* YouTube interview with Judge Facciola and Michael Arkfeld.[5] The ABA Commission on Ethics 20/20 issued "Revised Draft Resolutions for Comment — Technology and Confidentiality," in February 2012. Among other things, this draft adds to the Comments following Rule 1.1, under the heading **Maintaining Competence: "**[6] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with technology . . . ."[6] The emerging standard of care requires that integrated technical and legal expertise be brought to bear on issues involving electronically stored information, particularly where volumes are large, systems are complex, or there is legacy data to contend with.

Expertise and risk are likely inversely related to one another. But there are additional factors to weigh. For example, as noted above, there's the question of coverage. Will the law firm's professional liability insurance cover decisions it makes about data and document disposals? Would the carrier appreciate knowing that the partners don't carefully attend to post-litigation or post-representation file closure protocols and fail to address return, retention or disposal of the client's electronic data held in the law firm's (or third party vendor's) files? In addition, as noted above, documentation of the law firm's housecleaning is critical to a defensible process. How the firm staffs the work may have an impact on whether or not internal documents created during the project are subject to privilege protections.

For maximum protection, an insured and experienced legal expert should draft an opinion letter explaining the process and recommending the final disposition of unneeded data. No one internal to the organization is comfortable saying "throw it out", and litigation counsel may have difficulty convincing their clients to come to that decision. In the event that there is ever a challenge to the

---

[5] *See* Interview, <http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202543653146&John_Facciola_Michael_Arkfeld_on_the_ABA_Ethics_2020_Project_&slreturn=1> [visited April 22, 2012].

[6] *See also* ABA Model Rule of Ethics 1.1: "Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."

disposition of the data, the law firm – and its clients -- can point to this process and its associated documentation as evidence of their good faith effort to comply with its recordkeeping obligations. In addition, should data disposals be questioned in a litigation context, it is the consultant and not litigation counsel who should be subject to deposition. Shifting the burden in this way can be both effective and comforting for the law firm and its clients.

Anne Kershaw is the co-founder and president of the non-profit Electronic Discovery Institute (www.ediscoveryinstitute.org), which performs research and education on technologies and processes that intersect in some way with law. EDI's reports and articles are available for download from EDI's website free of charge. She is also the principal of A. Kershaw, PC// Attorneys & Consultants (www.AKershaw.com), a data and litigation management consulting firm, and is co-chair of the Subcommittee on e-Discovery and Litigation Technology of the Litigation Section's Committee on Corporate Counsel. Ms. Kershaw is also a faculty member of Columbia University's Master of Science in Information and Knowledge Strategy program. She can be contacted at Anne@AKershaw.com

Shannon Spangler is an attorney with more than 25 years' experience representing organizations in complex litigation. She is positioned to provide practical, strategic litigation counsel, bringing to every engagement her broad experience managing E-discovery, advising on records management best practices and data privacy issues, and counseling business executives regarding risk mitigation. Ms. Spangler was an associate and partner at Shook, Hardy & Bacon for 18 years and was managing partner of the firm's San Francisco office from 1999 – 2005. She was named one of San Francisco's "100 Most Influential Women in Business," San Francisco Business Week, May 2005. During her tenure as the office managing partner, the office received The Bar Association of San Francisco's 2004 "No Glass Ceiling" Award for its support of women in the profession. From 2005-2012, she served as Vice President and Associate General Counsel in the law department of a Fortune 500 company, responsible for compliance with the company's E-discovery obligations and for management of a portfolio of regulatory, commercial, intellectual property, and antitrust litigation. Email: Shannon@slspanglerpc.com.

E-Discovery's New Frontier: What the Increase in Portable Corporate Communication Means for E-Discovery

By Skye L. Perryman, Alexander B. Hastings, and Edward H. Rippey



Portable Electronic Devices (PEDs) -- such as BlackBerrys, iPads, and smart phones -- are crucial in modern business communication. It is now common corporate communications to occur via these devices, as opposed to face to face meetings or e-mails from desktop computers. The proliferation of PEDs raises several issues for the preservation and collection of electronic data in litigation and investigations required under the Federal Rules of Civil Procedure and state equivalents. Ensuring best practices relating to information stored on PEDs will become even more critical as the use of such devices expands.

This article begins by discussing the unique discovery challenges associated with increased use of PEDs, and then examines the emerging case law regarding legal obligations surrounding PEDs. We also discuss the practical burdens associated with preservation and collection of data on PEDs, and outline some best practices in this emerging area of e-discovery.

Unique E-Discovery Challenges of PEDs

As employees increasingly rely on PEDs as alternatives to desktop and laptop computer systems, recognizing unique challenges associated with these devices and creating solutions to respond to preservation and extraction obligations is as important as ever. While most e-discovery experts are familiar with the challenges accompanying data preservation in a tradition computer network system, PEDs raise different, but equally challenging, considerations. Before turning to general preservation obligations associated with these devices and the potential solutions to answer such obligations, it is important to consider a few of these unique challenges.

Lack of Standardized Storage Options: Text messages, e-mails, pictures, task lists and other data can be stored in several mediums on PEDs. Available storage options vary with each device and include internal flash memory, subscriber identity modules ("SIM cards"), cloud servers and in-house servers. The diversity of storage options presents unique challenges in the context of the need to preserve and extract material from these forms of storage.

Volatile State of Memory: In addition, many PEDs rely primarily on flash memory for storage similar to the RAM storage used by traditional computer systems. This flash memory provides a relatively inexpensive quick-access storage solution for text messages, e-mails, and other data on a PED, but its semi-persistent nature subjects data to potential overwriting. The volatile state of this data presents

challenges to preservation, which itself may not provide a defense to spoliation, even if the user never intended the data for long-term storage.[1]

Use of Personal Devices: The issues that arise with the various storage mediums and semi-persistent state of the memory in these devices are compounded by the difficulty of bringing these devices under the umbrella of an entity's data management policies. Specifically, unlike other electronic sources of information, often employees rely on personal devices that may not be linked to the entity's network. As a result, the information stored on these devices is not subject to the same level of control and preservation protections compared to traditional laptop and desktop systems operating on an entity's network.

Challenges Extracting Data: In addition to these issues that raise significant preservation concerns, PEDs also present unique challenges in extracting data. PEDs are marked by a greater lack of standardization, in terms of software and hardware, compared traditional computers and corporate networks. The lack standardization makes extraction of potentially responsive material difficult. For example, the Android operating system is generally regarded by collection experts as providing easier collection of data based on the open architecture of the operating system, especially compared to other PEDs. While the appropriate device will vary for each entity's unique situation, information technology professionals should give consideration to data extraction concerns when making decisions regarding these devices.

These four challenges -- the variety of storage mediums, the volatile state of PED memory, the use of personal devices, and the challenges extracting data -- require unique solutions, some of which are discussed below. Before considering the solutions, however, it is important to evaluate the preservation obligations imposed by courts concerning data on PEDs.

Overview of Preservation Obligations and Unsettled Legal Issues

Notwithstanding the common use of PEDs, case law specifically addressing preservation of data on PEDs is sparse and evolving. Although there are few reported federal cases that discuss preservation of data stored on PEDs, much of the existing case law can be applied to provide insight into the preservation obligations likely associated with data stored on these devices. Understanding and monitoring this area of the law is critical to ensuring continued compliance with discovery obligations. The Federal Rules of Civil Procedure and state equivalents, as well as the case law interpreting these authorities, generally require that electronically stored information ("ESI") potentially relevant to an actual or anticipated litigation be preserved. Courts have taken a broad view of the scope of data that consists of ESI and some cases have indicated that such data must be preserved even if stored on

[1] *See, e.g.*, *Columbia Pictures Inc. v. Bunnell*, 254 F.R.D. 443, 446 (C.D. Cal. 2007) (holding that information stored on volatile RAM must be preserved despite the party's intention that the information would never be stored on a long-term basis).

portable devices.[2] While much of this case law has developed in the context of civil discovery, the broad duty to preserve is also of crucial importance in criminal cases and investigations.

One of the first cases to address the discoverability of data stored on portable devices was *Smith v. Café Asia*, where the United States District Court for the District of Columbia held that images stored on a cell phone were discoverable (and relevant) to the underlying litigation.[3] More recently, courts have affirmed the duty to preserve relevant, unique data that is stored on portable devices and some have issued sanctions against parties for failing to preserve unique information stored on electronic devices. The most striking example of this can be found in the court's opinion in *Southeastern Mechanical Services v. Brody.* In *Brody*, a federal district court sanctioned a party for "wiping" unique data (text messages, calendar entries, e-mails) stored on a portable (blackberry) device that had not been preserved through backup tapes.[4] The court in *Brody* also noted that the wiping of data from a personal BlackBerry was improper because the party used the personal BlackBerry device for work during the relevant time period.[5] Along the same lines, in *Passlogix, Inc. v. 2FA Technology, LLC*, a court found that failing to preserve text and Skype messages constituted spoliation.[6] Aside from these and a few additional cases[7], there is not a large body of case law addressing preservation obligations a specifically applied to PEDs.

While the case law addressing data preservation on portable electronic devices is not as developed as those cases that concern e-mail or documents and information stored on a computer's harddrive, it is clear from the existing case law that courts are likely to find failure to preserve relevant and unique data on portable devices improper if no other copy of the data has been preserved. Less clear, however, is the length that courts will require litigants to go to preserve and collect data on PEDs, as such efforts could be burdensome given the state of data collection technology at this time. The law is also unsettled as to whether parties can successfully rely on the safe harbor provision in Rule 37(e) of the Federal Rules of Civil Procedure to justify an inadvertent failure to preserve data stored on portable devices.

Rule 37(e) provides that "[a]bsent exceptional circumstances, a court may not impose sanctions under these rules 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*." *See* Fed. R. Civ. P. 37(e) (emphasis added). One could argue that relying on the safe harbor provision in the context of PEDs encapsulates that which the Advisory Committee sought to accomplish through Rule 37(e). Specifically, in

---

[2] *See, e.g., Smith v. Café Asia*, 246 F.R.D. 19 (D.D.C. 2007); *Se. Mech. Servs. v. Brody*, 657 F. Supp. 2d 1293 (M.D. Fla. 2009).
[3] Prior to *Smith v. Café Asia*, in 2005, the United States District Court for the District of Maryland implicitly recognized discoverability of data on portable devices. *See Hopson v. City of Baltimore*, 32 F.R.D. 228 (D. Md. 2005)
[4] *Brody*, 657 F. Supp. 2d at 1302.
[5] *Id.* at 1301.
[6] *Passlogix, Inc. v. 2FA Tech., LLC*, 708 F. Supp. 2d 378,416, 423 (S.D.N.Y. 2010).
[7] *See, e.g.*, *Flagg v. Detroit*, 252 F.R.D. 346, 352-53 (E.D. Mich. 2008) (discussing the discoverability of text messages stored on PEDs and explaining the "text messages under consideration here fit comfortably within the scope of the materials that a party may request under Rule 34").

recommending Rule 37(e) the Advisory Committee recognized that (1) automated features in many electronic systems "automatically create, discard, or update information without specific direction from, or awareness of" system users; (2) "such automatic features are essential to the operation of electronic information systems"; and (3) "suspending or interrupting these features can be prohibitively expensive and burdensome."[8] The Advisory Committee, thus, recognized that although parties may take all reasonable measures to avoid destruction of potentially responsive material, certain technologies make the preservation of all material practically impossible. Indeed, the volatile nature and changing technology of PEDs suggest that these devices must often delete information without direction from the user, which is a necessary function to allow for continual fast access to data.

While the technological challenges of preserving data on these various devices, combined with their core function of providing quick access to information rather than archiving it, may provide a potential defense when information stored on these devices cannot be recovered, the willingness of court to accept a Rule 37(e) varies significantly.[9] Moreover, it is important to note that Rule 37(e) provides only a safe harbor, but it does not generally relieve parties of any independent preservation obligations. Thus, to the extent that a party had an obligation to preserve unique data on PEDs (and, as discussed above, it appears that courts will generally find such a duty), Rule 37(e) may provide limited utility as a defense. Whether a loss of information occurred in "good faith" for the purposes of Rule 37(e) depends, in part, on whether a party has complied with preservation duties imposed by independent sources of law, the court, or the agreement of the parties.[10] Therefore, an entity should take all reasonable efforts to preserve material stored on PEDs and consider relying on Rule 37(e)'s safe harbor protections only in the unfortunate event that material was inadvertently destroyed. Some of the efforts that may help a party comply with its discovery obligations with regard to these devices (and thus demonstrate "good faith") are outlined in the following section.

Over the next few years, we expect that the case law regarding preservation of data on storage devices will continue to evolve and therefore legal counsel should monitor the movement in this area.

---

[8] Advisory Comm. on the Federal Rules of Civil Procedure, Report of the Civil Rules Advisory Committee 83 (May 27, 2005), available at http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Reports/CV5-2005.pdf.

[9] *Compare Bootheel Ethanol Invs., L.L.C. v. SEMO Ethanol Co-op.*, No. 1:08-CV-59 SNLJ, 2011 WL 4549626, *4 (E.D. Mo., Sept. 30, 2011) (rejecting plaintiff'990s Rule 37(e) defense based on "a simple 'failure of technology'" and imposing an adverse inference sanction), *and Oklahoma, ex rel. Edmondson*, No. 05-CV-329-GKF-SAJ, 2007 WL 1498973, at *6 (N.D. Okla. May 17, 2007) ("The Court further advises the parties that they should be very cautious in relying upon any "safe harbor" doctrine as described in new Rule 37([e])."), *with Mintel Int'l Group, Ltd. v. Neergheen*, No. 08-cv-3939, 2010 WL 145786, at *8 (N.D. Ill. Jan. 12, 2010) (declining to impose sanctions where lost electronic data was a result of "typical computer usage" as opposed to a pattern of spoliation).

[10] *See, e.g.*, *Cannata v. Wyndham Worldwide Corp.*, No. 2:10-cv-00068-PMP-LRL, 2011 WL 3495987, *3 (D. Nev. Aug. 10, 2011) (explaining that the Advisory Committee's comments to Rule 37(e) require that parties disengage any automatic deletion feature of the computer systems in light of a litigation hold).

A Path Forward: Solutions and Best Practices for Preservation of Data on PEDs

After exploring the unique challenges presented by PEDs and establishing the duty to preserve responsive information on these devices, it may come as a relief that solutions exist to assist an entity in addressing discovery concerns. To that end, the following discussion presents proactive steps and potential defenses that may assist an entity in responding to its discovery obligations. While this list is not exhaustive and each entity's position requires unique solutions, the discussion below may contribute to an entity's response to its preservation obligations in this context.

Be Proactive: Before litigation is reasonably anticipated, and the duty to preserve arises, entities can take proactive steps to minimize potential liabilities that may otherwise arise as a result of failing to comply with discovery obligations *vis-à-vis* these devices. In particular, attorneys and IT personnel should work closely together to bring PEDs and the information stored on them under the umbrella of an entity's document retention policies. Several measures can be taken. For example, e-mails should not be downloaded onto and solely stored on these devices to the exclusion of other storage mediums. Instead, even if a PED stores a certain number of e-mails for quick access, a separate e-mail server, which is subject to an entity's document retention policy, should serve as the primary storage for e-mail messages. Further, employees should be discouraged from using personal devices to transact business.[11] These steps and others will help bring PEDs under the umbrella of an entity's already established document retention policy thereby helping to minimize the preservation concerns that arise as a result of the volatile nature of the storage on these devices. Nevertheless, the rapidly developing PED software and hardware platforms, combined with the growing number of individuals using personal devices to transact business, make it difficult to ensure that PEDs align with overall data management policies. As a result, other solutions must be explored.

Raise the Issue Early and Consider Stipulations: After litigation is reasonably anticipated and a duty to preserve arises, litigants should engage with opposing counsel early and often to discuss sources of potentially responsive material. Regardless of whether a party is requesting or producing information, such discussions are especially important when PEDs are involved. Parties requesting information should place the opposing party on notice of the need to preserve data on PEDs if the party has reason to believe that responsive material may be located on these devices. Further, a party faced with the need to produce material should evaluate whether PEDs within its control, or the control of its agents, may contain responsive material. A producing party assessing the amount and value of potentially responsive material stored on PEDs should consider whether an undue burden argument can be made to the court or the opposing party when negotiating discovery obligations. Even if an undue burden

[11] The likelihood remains significant that individuals will use personal devices for business purposes outside an entity's data management policies. For example, several surveys suggest that approximately fifty percent of employees reported using their personal devices for business purposes. *See* Jeff Fehrman, *Mobile Devices: A Singular Threat to Corporate Compliance and E-Discovery*, CORPORATE COMPLIANCE INSIGHTS (May 31, 2012), http://www.corporatecomplianceinsights.com/mobile-devices-a-singular-threat-to-corporate-compliance-and-e-discovery/

argument may be made, however, some courts remain skeptical of such an argument in the context of PEDs.[12]

Parties should also assess whether the data stored on PEDs is unique, or whether it is merely a copy of data that exists on active servers. If the later, it is possible that copies of the data need not be preserved on PEDs. However, caution should be taken when assessing duplicative data, as, should the data not be duplicative, a court would likely find a legal obligation to preserve the unique data on the PED.

As part of these discussions, it can also be useful to attempt to reach agreement with opposing counsel on the scope of discovery, including the scope of preservation and collection that they expect from portable devices. We have found such stipulations to be helpful in reducing the burden on the producing party to collect and preserve data on portable devices. Some stipulations may limit the preservation and collection of data on PEDs altogether, while others might only require preservation and collection of data on PEDs from "key players." Stipulations can lend a great deal of flexibility and certainty to this relatively unsettled area of the law. Nevertheless, it is important to check local rules and practices with regard to party stipulations, as some courts may require that any such agreements -- in order to have effect in the case -- be entered by the court.

Consider Early Data Extraction: After identifying that litigation is reasonably anticipated and PEDs contain potential responsive material, a party may want to consider extracting data early. As noted, the lack of standardization in the hardware and software of PEDs can make extraction of potentially responsive data particularly burdensome. Early extraction can be important, however, because the volatile nature of these devices requires that a party take action to preserve material to minimize the potential for spoliation. Luckily, many e-discovery vendors are able to assist parties in their collection of data from these devices. Forensic Toolkit and EnCase Forensic are two examples of data collection platforms that provide support for extraction of data from PEDs. While the appropriate collection solution for any particular entity may vary, it is worth noting that vendors are responding to the need to extract data from these devices and such tools can assist entities in ensuring that early extraction occurs.

Develop a Defensible Position and Record of Good Faith: Despite undertaking reasonable efforts to preserve and extract data on PEDs, the volatile storage conditions of these devices can result in the loss of potentially relevant material. As a result, parties may be faced with defending against a motion for sanctions based on spoliation. As noted above, in this circumstance, a party can rely on the safe harbor provision in Federal Rule of Civil Procedure 37(e); however, it is far from certain that a court will

[12] *See, e.g.*, *Treppel v. Biovail*, 233 F.R.D. 363, 372 (S.D.N.Y. 2006) (Denying motion for protective order for "electronic data including email data . . . on PDA's [and] Blackberries" because the plaintiff had not demonstrated the devices did not contain relevant material).

use its discretion to excuse any data destruction and taking the steps outlined above may help demonstrate "good faith" in the event that such data is destroyed inadvertently.

Conclusion

While the use of PEDs is common, the case law in this area is evolving. Nevertheless, based on the current case law, courts will likely require parties to preserve unique, relevant information stored on PEDs -- and, absent a stipulation or other agreement, parties therefore should take early efforts to ensure that such information is preserved.

Skye Perryman (sperryman@cov.com) is a litigation associate at Covington & Burling, LLP in Washington, D.C and a member of the E-Discovery Practice Group. Alexander Hastings (ahastings@cov.com) is a litigation associate at the firm and is a member of the E-Discovery Practice Group. Edward Rippey (erippey@cov.com) is a partner at the firm, handles complex commercial litigation, and is Chair of the E-Discovery Practice Group.

Five Proportionality Principles That Can Reduce eDiscovery Costs and Burdens

By Philip Favro

Talk to most any enterprise about legal issues and invariably the subject of eDiscovery will come up as a thorny pain point. These discussions typically focus on the high costs of eDiscovery, particularly for data preservation and document review. Such costs and the inevitable delays that accompany the discovery process provide ample justification for organizations to be on the alert for ways to address these issues.

As a solution to these costs and delays, the eDiscovery cognoscenti are emphasizing the concept of "proportionality." Proportionality typically requires that the benefits of discovery be commensurate with its corresponding burdens.[1] Under the Federal Rules of Civil Procedure (Rules), the directive that discovery be proportional is found in Rule 26. In what may be a surprise to some practitioners, Rule 26(b)(2)(C) empowers courts to restrict the liberal bounds of federal discovery practice. For example, discovery *must* be limited where requests are unreasonably cumulative or duplicative, the discovery can be obtained from an alternative source that is less expensive or burdensome, or the burden or expense of the discovery outweighs its benefit.[2]

This provision is reinforced by Rule 26(g), which imposes an express certification obligation on counsel to engage in proportional discovery or face sanctions.[3] An additional proportionality provision specific to eDiscovery is found in Rule 26(b)(2)(B). That rule limits the discovery of electronically stored information (ESI) such as backup tapes that may not be "reasonably accessible because of undue burden or cost."[4] Finally, Rule 26(c) provides an enforcement mechanism for these provisions. Parties may seek protective orders under this provision, which limits or even proscribes discovery that causes "annoyance, embarrassment, oppression, or undue burden or expense."[5]

While proportionality standards were underused for years after they were first included in the Rules, they are now being championed by various district and circuit courts. As more opinions are issued that analyze proportionality, several key principles are becoming apparent in this developing body of jurisprudence. To better understand these principles, it is instructive to review some of the top proportionality cases issued this year and last. These cases and the proportionality standards they espouse provide a roadmap of best practices which, if followed, will help courts, clients and counsel reduce the costs and burdens of eDiscovery.

---

[1] Eisai Inc. v. Sanofi-Aventis U.S., LLC, No. 08–4168 (MLC), slip op. at 6 (D.N.J. Apr. 16, 2012) (invoking proportionality standards to deny the majority of plaintiff's production requests).
[2] Fed.R.Civ.P. 26(b)(2)(C).
[3] Fed.R.Civ.P. 26(g).
[4] Fed.R.Civ.P. 26(b)(2)(B).
[5] Fed.R.Civ.P. 26(c).

Encourage Reasonable Discovery Efforts

The first of these cases, *Larsen v. Coldwell Banker Real Estate Corp.*, emphasizes that discovery efforts need only satisfy a standard of reasonableness, not perfection.[6] In *Larsen*, the court rejected the plaintiffs' assertion that the defendants should be made to redo their production of documents. The plaintiffs had argued that doing so was necessary to address certain discrepancies – including missing emails – in the defendants' production. The court disagreed, holding instead that plaintiffs had failed to establish that such discrepancies had prevented them from obtaining relevant information.[7]

The court also reasoned that a "do over" would violate the principles of proportionality codified in Rule 26(b)(2)(C). After reciting the proportionality language from Rule 26, the court determined that "the burden and expense to Defendants in completely reproducing its entire ESI production far outweighs any possible benefit to Plaintiffs."[8] There were simply too few discrepancies identified to justify the cost of redoing the production.

The *Larsen* decision provides a reminder that organizations' discovery efforts need not be perfect. The Rules were never intended to exact perfection in the discovery process. That misguided understanding of federal discovery practice has spawned too many expensive and futile eDiscovery sideshows.[9] Instead, the parties' efforts must be reasonable such that the overall purposes of discovery can be fulfilled.[10]

Discourage Unnecessary Discovery

The next case underscores the corollary principle of discouraging unnecessary discovery. In *Bottoms v. Liberty Life Assur. Co. of Boston*, the court drastically curtailed the written discovery that plaintiff sought to propound on the defendant.[11] Plaintiff had requested leave in this ERISA action to serve "sweeping" interrogatories and document requests to resolve the limited issue of whether the defendant had improperly denied her long term disability benefits. Drawing on the proportionality standards under Rule 26(b)(2)(C), the court characterized the proposed discovery as "patently overbroad" and as seeking materials that were "largely irrelevant."[12] The court ultimately ordered the defendant to respond to some aspects of plaintiff's interrogatories and document demands, but not before limiting their nature and scope.

---

[6] Larsen v. Coldwell Banker Real Estate Corp., No. SACV 10–00401–AG (MLGx) (C.D. Cal. Feb. 2, 2012).
[7] *Id*. at 7.
[8] *Id*. at 8.
[9] *See* Brigham Young University v. Pfizer, Inc., No. 2:06–cv–890 TS, slip op. (D. Utah Apr. 16, 2012) (denying plaintiffs' fourth motion for "doomsday" sanctions since evidence was destroyed pursuant to defendants' "good faith business procedures").
[10] *See, e.g.*, United States v. Procter & Gamble Co., 356 U.S. 677, 682 (1958) (reasoning that discovery is intended to "make a trial less a game of blind man's buff and more a fair contest with the basic issues and facts disclosed to the fullest practicable extent); Hickman v. Taylor, 329 U.S. 495, 501 (1947) (opining that a key purpose for civil discovery is to "narrow and clarify" the issues in dispute).
[11] Bottoms v. Liberty Life Assur. Co. of Boston, No. 11–cv–01606–PAB–CBS, slip op. (D. Colo. Dec. 13, 2011).
[12] *Id*. at 10.

The *Bottoms* case emphasizes what courts have been urging for years: that organizations should do away with unnecessary discovery. This typically requires counsel to steer away from boilerplate demands or "robotically recycling" requests from previous lawsuits.[13] Instead, lawyers should "stop and think" about what discovery is actually needed and then prepare well tailored requests.[14] For as *Bottoms* teaches, the obligation to ensure that discovery is both reasonable and proportional principally rests with the parties and their counsel.

Encourage Defensible Deletion of ESI

Another recent proportionality decision demonstrates the importance of defensibly deleting ESI, particularly for preservation purposes. In *Grabenstein v. Arrow Electronics*, the court refused to sanction a company for eliminating emails pursuant to a good faith document retention policy.[15] The plaintiff had argued that drastic sanctions (evidence, adverse inference and monetary) should be imposed on the company since relevant emails regarding her alleged disability were not retained in violation of an EEOC retention requirement. The court rejected that argument, finding that sanctions were inappropriate because the emails were overwritten pursuant to a reasonable data retention policy before the common law preservation duty was triggered.[16]

The court also reasoned that sanctions would be inappropriate since plaintiff managed to obtain the destroyed emails from a third party.[17] Without expressly mentioning "proportionality," the court implicitly drew on the "other source" language from Rule 26(b)(2)(C) to reach its "no harm, no foul" approach. Given that plaintiff actually *had* the emails in question and there was no evidence suggesting other ESI had been destroyed, proportionality standards tipped the scales against sanctioning the company for not observing a regulatory retention norm.

The *Grabenstein* case reinforces the notion that a party's preservation obligations must be analyzed through the lens of reasonableness and proportionality.[18] In addition, *Grabenstein* teaches organizations to develop and then follow reasonable retention policies that eliminate data stockpiles before litigation is reasonably anticipated.[19] It also demonstrates the value of deploying a timely and comprehensive litigation hold to ensure that relevant ESI is retained once a preservation duty is

[13] *Id*. at 5.
[14] *Id*.
[15] Grabenstein v. Arrow Electronics, No. 10-cv-02348-MSK-KLM, slip op. (D. Colo. Ap. 23, 2012).
[16] *Id*. at 4.
[17] *Id*. at 6.
[18] *See* Pippins v. KPMG LLP, --- F.R.D. ---- (S.D.N.Y. 2012) (explaining that "proportionality is necessarily a factor in determining a party's preservation obligations").
[19] *See* Micron Technology, Inc. v. Rambus Inc., 645 F.3d 1311 (Fed.Cir. 2011) (approving corporate retention policies adopted for "good housekeeping" purposes).

triggered.[20] By following these "good faith business procedures," organizations can establish a defensible information governance plan that is consistent with principles of proportionality.

Encourage Cooperation in Discovery

The *Pippins v. KPMG* case exemplifies how proportionality also encourages litigants to cooperate in discovery.[21] In *Pippins*, the court ordered the defendant accounting firm to preserve thousands of employee hard drives. The firm had argued that the high cost of preserving the drives was disproportionate to the value of the ESI stored on the drives. Instead of preserving all of the drives, the firm hoped to maintain a reduced sample, asserting that the ESI on the sample drives would satisfy the evidentiary demands of the plaintiffs' class action claims.

The court rejected the proportionality argument primarily because the firm refused to permit plaintiffs or the court to analyze the ESI found on the drives.[22] Without any transparency into the contents of the drives, the court could not weigh the benefits of the discovery against the alleged burdens of preservation. The court was thus left to speculate about the nature of the ESI on the drives, reasoning that it went to the heart of plaintiffs' class action claims. As the court caustically noted, the firm may very well have obtained the relief it requested had it engaged in "good faith negotiations" with plaintiffs over the preservation of the drives.[23]

The *Pippins* decision reinforces a common refrain that proportionality is generally available to those parties who have engaged in reasonable, cooperative discovery conduct. Staking out unreasonable positions in the name of zealous advocacy stands in stark contrast to the clear trend that discovery should comply with the cost cutting mandate of Rule 1.[24] Cooperation and proportionality are two of the principal touchstones for effectuating that mandate. As *Pippins* demonstrates, the failure to cooperate may very well foreclose proportionality considerations.

Encourage Better Information Governance Practices

Proportionality also encourages organizations to think ahead and develop effective information governance practices, a point emphasized in *Salamone v. Carter's Retail, Inc*.[25] In *Salamone*, the court denied a motion for protective order that the defendant retailer filed to stave off the collection of thousands of personnel files. The retailer had argued that proportionality precluded the search and review of the personnel files. In support of its argument, the retailer asserted that the nature, format, location and organization of the records made their review and production too burdensome: "the burden of production . . . outweigh[s] any benefit to plaintiffs considering the disorganization of the

[20] *See* Viramontes v. U.S. Bancorp, No. 10 C 761, slip op. (N.D. Ill. Jan. 27, 2011) (denying sanctions motion since defendant, among other things, issued a timely litigation hold to preserve relevant documents once a preservation duty attached).
[21] Pippins v. KPMG LLP, --- F.R.D. ---- (S.D.N.Y. 2012).
[22] *Id*. at 12.
[23] *Id*. at 9.
[24] Fed.R.Civ.P. 1.
[25] Salamone v. Carter's Retail, Inc., No. 09-5856 (GEB), slip op. (D.N.J. Jan. 28, 2011)

information, the lack of accessible format, the significant amount of labor and costs involved, and defendant's management structure."[26]

In rejecting the retailer's position, the court identified its information retention system as the culprit for its burdens. That the retailer, the court reasoned, "maintains personnel files in several locations without any uniform organizational method does not exempt Defendant from reasonable discovery obligations."[27] After weighing the various factors that comprise the proportionality analysis under Rule 26(b)(2)(C), the court concluded that the probative value of production outweighed the resulting burden and expense on the retailer.

Having an intelligent information governance process in place could have addressed the cost and logistics headaches that the retailer faced. Had the records at issue been digitized and maintained in a central archive, the retailer's collection burdens would have been significantly minimized. Furthermore, integrating these "upstream" data retention protocols with "downstream" eDiscovery processes could have expedited the review process. The *Salamone* case teaches that an integrated information governance process, supported by effective, enabling technologies, will likely help organizations reach the objectives of proportionality by reducing discovery burdens and making them more commensurate with the demands of litigation.

Conclusion

The foregoing cases exemplify how proportionality standards can help lawyers and litigants conduct eDiscovery in an efficient and cost effective manner. By faithfully observing these principles, organizations truly stand a better chance of conducting litigation in a "just, speedy, and inexpensive" manner.[28] This will ultimately succeed in reducing the costs and burdens of litigation.

Philip Favro is Discovery Counsel for Symantec Corporation in Mountain View, California. During his eleven-year litigation practice, he advised technology companies and other clients regarding complex discovery issues. Phil's expertise has been enhanced by his legal scholarship. His line of research addresses the changes and challenges that electronic data have forcibly introduced into litigation and, in particular, on discovery practice. He now works with Symantec customers and company stakeholders on information governance and discovery matters.

Phil has been a member of the California State Bar since 1999 and is also licensed to practice in Utah. He belongs to the American Bar Association and is a member of the ABA's Science & Technology Section. He is a member of The Sedona Conference and contributes to Working Groups 1 and 6. He previously chaired the Santa Clara County (California) Bar Association's High Technology Law Section and was a member of its Board of Trustees. Phil also serves as a Judge Pro Tempore for the Santa Clara County Superior Court based in Santa Clara, California.

[26] *Id*. at 6 (internal quotations removed).
[27] *Id*. at 12.
[28] Fed.R.Civ.P. 1.

Editor's Message

Now well into the third year of publication, this issue of the *EDDE Journal* presents articles from lawyers in various-sized law firms and in corporations. The first article from John Isaza is the second part of his article on information management, this time focusing on the standards and principles for records and information management that underlie the Generally Accepted Recordkeeping Principles. This is based on a compilation created by Ms. Helen Streck, the CEO of Kaizen InfoSource, LLC. The second article is from Anne Kershaw and Shannon Spangler, the second time for Anne and first time for Shannon. This article analyzes the issue of law firms' retention of their client's information and the implications therein for subsequent litigation. The third article is from the lawyers at frequent contributors Covington & Burling, LLP led by Edward Rippey, authoring with Skye Perryman and Alexander Hastings. This discusses the very timely topic of preservation and collection of data on Portable Electronic Devices. The fourth article is from Philip Favro of Symantec, with his second article in the *EDDE Journal*. This article covers five principles of proportionality to help control the costs of e-discovery. Thank you to all of the authors for their submissions.

The EDDE committee's e-discovery workshops, pre-RSA meetings, the webinars, other face-to-face meetings, and other educational and professional activities are best located on the committee's website and listserv. You will also find the prior issues of this publication there. Please join the committee and volunteer for one of its many activities if you have not already done so.

I continue to ask that all readers of the *EDDE Journal* to share with their fellow professionals and committee members by writing an article for this periodical. Our next issue (Autumn 2012) will come out in September, 2012. There are many of you who have not yet been able to share your experience and knowledge through publishing an article here but please consider doing so to widen the understanding of all of our readers. Every qualified submission meeting the requirements explained in the Author Guidelines will be published, so please feel free to submit your articles or ideas, even if you are not quite ready for final publication. The issue after Autumn (Winter 2013) will be published in December 2012. Until then.