



**Tuesday, October 20**  
**9:00 am–10:30 am**

## **905 Ediscovery Tool Kit 1: Preparations, New Technologies & Discovery Management**

**Joseph J. Catalano**

*Senior Vice President and Chief Litigation Counsel*

Union Bank, N.A.

**Mark Diamond**

*Chief Executive Officer*

Contoural

**Patrick Oot**

*Director of Electronic Discovery and Senior Litigation Counsel*

Verizon

## Faculty Biographies

### **Joseph J. Catalano**

Joseph J. Catalano serves as senior vice president and chief litigation counsel for Union Bank in San Francisco. Previously he was the general counsel of Bay View Capital Corporation.

He has served as the chair of ACC's Litigation Committee and was chosen as the Member of the Year at the 2006 Annual Meeting of ACC. He is also a past president of ACC's San Francisco Bay Area Chapter. He currently serves on the chapter's board of directors and is co-chair of its litigation committee. He is the immediate past president of the San Francisco Bank Attorneys Association. Mr. Catalano is an advisory member of the Financial Institutions Committee of the State Bar of California. He is a frequent speaker and has spoken at the 2007 Annual Conference of the California Bankers Association and at its 2006 Annual Conference. He has presented on the topic of Records Management to the 2006 Annual Meeting of the Hispanic National Bar Association. His article, "Tips and Insights on: Litigation Management for Small Law," appeared in the March 2006 *ACC Docket*.

He received his bachelors from Manhattan College in New York, and his JD from University of the Pacific, McGeorge School of Law in California.

### **Mark Diamond**

Mark Diamond is founder and CEO of Contoural, Inc. As one of the industry thought leaders in proactive litigation readiness, compliance, records management and data archiving strategies he and his organization work with Fortune 500 companies, as well as many midsized and smaller organizations. Focusing on moving from reactive litigation response to proactive litigation readiness, he helps organizations set up comprehensive records information management programs from policy development to implementation. This includes ESI data mapping, change management as well as technology selection.

Previously Mr. Diamond founded Veritas' (now Symantec's) professional services group and founded and ran worldwide services for Legato Systems (now EMC).

Mr. Diamond is a frequent industry speaker and has written numerous articles.


Mr. Diamond is a graduate of the University of California San Diego and is currently a trustee of its Foundation.

**Patrick Oot**

Patrick Oot is director of electronic discovery and senior litigation counsel at Verizon in Washington, DC. Mr. Oot is charged with advising Verizon's business units on electronic discovery while developing new technologies that increase cost-efficiency.

Mr. Oot has appeared with United States Supreme Court Justice Stephen Breyer at Georgetown University Law Center's Summit on Electronic Discovery. He has testified before the United States Judicial Conference's Advisory Committee on the Federal Rules of Evidence where he presented Verizon's position on Proposed Rule of Evidence 502. The Committee included in its draft to the Judicial Conference language incorporating Mr. Oot's suggestions. Mr. Oot lectures regularly at educational events, legal conferences, and general counsel round tables internationally.

He received both his BA and JD from Syracuse University and his LLM from Georgetown University Law Center.



**Before Written Language...  
But We've Always Had Vendors**

So, Here's a Little History of Written Language

- *Hieroglyphics...Hard to Produce in Litigation*
- *Records Just Won't Go Away.*

2009 Annual Meeting  
October 18-21 Boston

*Don't just survive. Thrive!*

---

---

---


---

---

---

---

---



- Printing Press - About 500 Years Ago
- And then in 1965... Photocopying The Early Version...
- And we thought paper was bad...

2009 Annual Meeting  
October 18-21 Boston

*Don't just survive. Thrive!*

---

---

---


---

---

---

---

---



**Paper or ESI?**

- **The Sedona Principles** - authority on best practices and principles for addressing electronic document production. identify six ways in which ESI differs from paper documents:
  1. the enormous volume and duplicability of ESI;
  2. its persistence (ESI survives many efforts to "delete" it);
  3. its dynamic and changeable content;
  4. metadata associated with electronically stored "documents";
  5. the environment-dependence and obsolescence of ESI;
  6. the dispersion and searchability characteristics of ESI.

2009 Annual Meeting  
October 18-21 Boston

*Don't just survive. Thrive!*

---

---

---

---

---

---

---

---



**WAR ROOM!! aka**  
The Place Your Lawyers Beat Up Your Bank [small lawsuit]

**WAR ROOM!! Bigger Lawsuit...**

2009 Annual Meeting  
October 18-21 Boston

*Don't just survive. Thrive!*

---

---

---

---

---

---

---

**Lessons Learned 2008 to 2009...**

- "Reasonably" accessible standard further eroded to include more ESI Mancia v. Mayflower Textile Services Co., 2008 WL 4595275 (D. Md. Oct. 15, 2008)
- Aggressive regulators are creative with e-discovery tactics Grand Jury Charges in U.S. v. Cioffi and Tanno (Bear Stearns Investigation) (E.D.N.Y. Unpublished)
- The duty to preserve potentially relevant materials may be triggered before a lawsuit is filed Micron v. Rambus, 255 F.R.D. 135 (D. Del. 2009)
- In-house counsel can't just let outside counsel or e-discovery vendor take off with a case Qualcomm v. Broadcom, 2008 WL 638108 (S.D. Cal., Mar. 5, 2008)
- Search methodology should be "well reasoned" and discovery protocol must be well documented during the meet-and-confer stage Victor Stanley v. Creative Pipst, 2008 WL 2221841 (D. Md. May 29, 2008)
- Systematic failure to preserve and produce relevant evidence will likely lead to sanctions Keithley v. The Home Store.com, 2009 WL 816429 (N.D. Cal. Jan. 7, 2009)

2009 Annual Meeting  
October 18-21 Boston

*Don't just survive. Thrive!*

---

---

---

---

---

---

---

---

---

---

---

---

**e-Discovery Challenges – Fall 2009**

- Internal Challenges
  - Working with a reactive IT organization
  - New media – Blogs, Twitter, Texting
  - Time to grow up – getting away from ad hoc processes
  - Chevy vs. Cadillac litigation readiness
  - Justifying in-house counsel headcount
  - Building business case for senior management
- External Challenges
  - Fear of discovery and need for early case assessment
  - Diversity of discovery protocols
  - Controlling outside e-discovery firms
  - Managing overly broad outside counsel

2009 Annual Meeting  
October 18-21 Boston

*Don't just survive. Thrive!*

---

---

---

---

---

---

---

---

---

---

---

---

**What Are Others Doing for Litigation Readiness?**

Activity	Deployed (%)	Planned (%)
Create Three-Year Strategic Plan	~60	~80
Update Document Retention Policy	~80	~90
Develop E-mail and Data File Plans	~70	~85
Update Litigation Hold Policy	~75	~85
Update Litigation Hold Process	~55	~75
Create ESI Data Map	~25	~65
Enable Document Deletion Process	~20	~55
Deploy E-mail Archiving System	~45	~80
Deploy Data Search/Archiving Sys	~20	~45
Deploy Litigation Man. System	~15	~40
Create Records Management Org	~15	~55

Survey of large, midsize and small U.S. corporations actively improving litigation readiness from Oct. '08 - Sept. '09. Source: Contoural, Inc.

2009 Annual Meeting  
October 18-21 Boston

*Don't just survive. Thrive!*

---

---

---

---

---

---

---

---

---

---

---

---

ACC Association of Corporate Counsel

### Careful About Defining Problem Too Narrowly

2009 Annual Meeting  
October 18-21 Boston  
Don't just survive. Thrive!

---

---

---

---

---

---

---

---

ACC Association of Corporate Counsel

### Caution: Aggressive Deletion Drives Underground Archiving

*"The hot temper leaps over the cold decree."  
(Shakespeare, Merchant of Venice)*

2009 Annual Meeting  
October 18-21 Boston  
Don't just survive. Thrive!

---

---

---

---

---

---

---

---

ACC Association of Corporate Counsel

### Can Technology Alleviate the Pain?

Technology	Current Maturity	Current Adoption for Litigation Readiness	Cost to Purchase	Effort to Implement	Pain Threshold to Trigger Deployment	Impact on Alleviating Pain
E-mail Archiving	Medium	Medium	\$\$ to \$\$\$	Significant	Low to medium	High for control, cost containment
File Archiving/Search	Low to Medium	Low	\$ to \$\$\$	Easy to Moderate	Both cost and risk	High if search is an issue, low if cost
Litigation Management System	Low	Low	\$\$	Moderate to Significant	High volume of matters or \$\$ in settlements	High impact
Enterprise Content Management	High	Low	\$\$\$\$	Significant	Contracts, Patent IP biggest drivers	Medium impact for retention
Network based Collection Systems	Medium	Low	\$\$ to \$\$\$	Medium	High volume of matters or custodians	High impact on 3 <sup>rd</sup> party e-discovery
In House Review Tools	Medium	Low	\$\$	Easy	Settlements due to unknown, high review costs	High impact on 3 <sup>rd</sup> party e-discovery

2009 Annual Meeting  
October 18-21 Boston  
Don't just survive. Thrive!

---

---

---


---

---

---

---

---

 **Archiving Really Isn't About Saving...**

- What do you have? Where is it?
- Can you search documents? Can you retrieve documents?
- Can you save documents that are "business records"?
- Can you preserve the right documents in the event of litigation? Can you avoid saving non-relevant documents?
- Do you delete documents you don't need?
- Can you do this consistently, defensibly, and cost effective?

Policies + Processes + Tools + Training = **CONTROL**

2009 Annual Meeting  
October 18-21 Boston

*Don't just survive. Thrive!*

---

---

---


---

---

---

---

---

 **2009 – 2010:  
Re-empowering In-House Counsel**

- Don't simply hand over reigns to outside counsel, vendors or IT
- Better upstream management and hold processes drive downstream defensibility and cost savings
- Data control isn't only Legal's issue
- Technology works if applied selectively and effectively
- Data archiving is good, but consistent archiving and automated deletion is better

2009 Annual Meeting  
October 18-21 Boston

*Don't just survive. Thrive!*

---

---

---

---

---

---

---

---



**ACC** Association of Corporate Counsel

**Corporate Counsel Empowerment Skills and Tools**

Consider **Litigation Strategies**:

- Cooperation
- Negotiation
- Effective Protective Orders
- FRE 502

2009 Annual Meeting  
October 18-21 Boston

*Don't just survive. Thrive!*

---

---

---

---

---

---

---

---

---

---

---

---

**ACC** Association of Corporate Counsel

**FRCP Rule 1**

– **These rules govern the procedure in all civil actions and proceedings in the United States district courts, except as stated in Rule 81. They should be construed and administered to secure the just, speedy, and inexpensive determination of every action and proceeding.**

2009 Annual Meeting  
October 18-21 Boston

*Don't just survive. Thrive!*

---

---

---

---

---

---

---

---

---

---

---

---

Hon. Richard A. Frye  
 Franklin County Court of Common Pleas  
 Columbus, OH  
 Hon. Kathleen McDonald O'Malley  
 U.S. District Court for the Northern District of Ohio  
 Cleveland, OH  
 OREGON  
 Hon. Robert DeBarack  
 U.S. District Court for the Western District of Oklahoma  
 Oklahoma City, OK  
 Hon. Robin J. Coulson

**The Sedona Conference® Cooperation Proclamation  
Judicial Endorsements as of January 20, 2009**

WASHINGTON  
 Hon. Barbara Seiber Matheson  
 U.S. District Court for the Western District of Washington  
 Seattle, WA

---

---

---

---

---

---

---

---

---

---

---

---

ACC Association of Corporate Counsel

Cases Citing The Sedona Conference® Cooperation Proclamation

**Covad Communications Company v. Revonet, Inc.**  
354 F.R.D. 147 (D.D.C. Dec. 31, 2008)

**William A. Gross Construction Associates, Inc. v. American Manufacturers Mutual Insurance Co.**  
2009 WL 724954 (S.D.N.Y. 2009)

**Newman v. Borders**  
2009 WL 931545 (D.D.C. 2009)

**Mancia v. Mayflower Textiles Servs. Co.**  
253 F.R.D. 354 (D. Md. Oct. 15, 2008)

**SEC v. Collins & Aikman Corp.**  
2009 WL 94311 (S.D.N.Y. 2009)

**Aguilar v. Immigration and Customs Enforcement Division of the U.S. Dept. of Homeland Security**  
255 F.R.D. 350 (S.D.N.Y. 2008)

**William Gipson v. Southwestern Bell Telephone Company**  
2008 U.S. Dist. LEXIS 103822 (Dec. 2008)

2009 Annual Meeting  
 October 18-21 Boston

*Don't just survive. Thrive!*

---

---

---

---

---

---

---

---

---

---

---

ACC Association of Corporate Counsel

**Reasons to Cooperate**

2009 Annual Meeting  
 October 18-21 Boston

*Don't just survive. Thrive!*

---

---

---

---

---

---

---

---

---

---

---

ACC Association of Corporate Counsel

**Do you really want the judge to manage discovery?**

**Newman v. Borders**  
2009 WL 931545 (D.D.C. 2009)

2009 Annual Meeting  
 October 18-21 Boston

*Don't just survive. Thrive!*

---

---

---

---

---

---


---

---

---

---

---



**Cooperating is the ethical thing to do.**

**William A. Gross. Constr. Assocs., Inc. v. Am. Mfrs. Mut. Ins. Co.,**  
2009 WL 724954 (S.D.N.Y. Mar. 19, 2009)

2009 Annual Meeting  
October 18-21 Boston

*Don't just survive. Thrive!*

---

---

---


---

---

---

---

---



**The Rules Require Cooperating.**

**Mancia v. Mayflower Textile Servs. Co.,**  
253 F.R.D. 354 (D. Md. 2008)

2009 Annual Meeting  
October 18-21 Boston

*Don't just survive. Thrive!*

---

---

---


---

---

---

---

---



**Cooperating is less expensive.**

**In re Fannie Mae Sec. Litig.,**  
552 F.3d 814 (D.C. Cir. 2009)

2009 Annual Meeting  
October 18-21 Boston

*Don't just survive. Thrive!*

---

---

---

---

---

---

---

---

ACC Association of Corporate Counsel

**Cooperating Avoids Sanctions.**

**Bray & Gillespie Mgmt. LLC v. Lexington Ins. Co.**  
2009 WL 546429 (M.D. Fla. Mar. 4, 2009)

2009 Annual Meeting  
October 18-21 Boston

*Don't just survive. Thrive!*

---

---

---

---

---

---

---

---

ACC Association of Corporate Counsel

**Cooperating Can Protect Privilege and Save Costs**

**Federal Rule of Evidence 502**

2009 Annual Meeting  
October 18-21 Boston

*Don't just survive. Thrive!*

---

---

---

---

---

---

---

---

ACC Association of Corporate Counsel

**FRE 502: Case Law Discussion**

*FRE 502 Article:  
The Sedona Conference Journal  
Fall 2009*

2009 Annual Meeting  
October 18-21 Boston

*Don't just survive. Thrive!*<sup>12</sup>

---

---

---

---

---

---

---

---

**ACC** Association of Corporate Counsel

**Rhoads Industries, Inc. v. Building Materials Corp., 2008 WL 4916026 (E.D. Pa. 2008).**

- Applied FRE 502 and 5-factor *Fidelity* test to find that no waiver existed for the documents in question.
- Interests of justice favored the plaintiffs, especially since defendants had no expectation of receiving the documents at issue.
- Disagrees with "after-the-fact critique" in *Victor Stanley*.
- But cautions that "[a]n understandable desire to minimize costs of litigation and to be frugal in spending a client's money cannot be an after-the-fact excuse for a failed screening of privileged documents. ..."

2009 Annual Meeting  
October 18-21 Boston

*Don't just survive. Thrive!*

---

---

---

---

---

---

---

---

---

---

---

---

**ACC** Association of Corporate Counsel

**Alcon Mfg., Ltd. v. Apotex, Inc., 2008 WL 5070465 (S.D. Ind., Nov. 26, 2008).**

- Plaintiffs inadvertently produced document that was included on their privilege log but produced due to an electronic document break error.
- Considering newly-enacted FRE 502, court found that the waiver issue was determined by the parties' stipulated protective order entered prior to discovery, which required the return of inadvertently-produced attorney-client communications.
- Court found that plaintiffs had performed a diligent review of their documents prior to their production and responded reasonably quickly upon notice that the privileged document had been inadvertently produced. Privilege was not waived because plaintiffs had complied with the stipulated protective order.
- "Perhaps the situation at hand could have been avoided had Plaintiffs counsel meticulously double or triple-checked all disclosures against the privilege log prior to any disclosures. However, this type of expensive, painstaking review is precisely what new Evidence Rule 502 and the protective order in this case were designed to avoid."

2009 Annual Meeting  
October 18-21 Boston

*Don't just survive. Thrive!*

---

---

---

---

---

---

---

---

---

---

---

---

**ACC** Association of Corporate Counsel

**SEC v. Badian, 2009 WL 222783 (S.D.N.Y, Jan. 26, 2009).**

- Applied factors identified in *Louis Sportswear, U.S.A., Inc. v. Levi Strauss & Co., 104 F.R.D. 103, 105 (S.D.N.Y. 1985)* and its progeny to conclude that non-party Rhino waived any claim of privilege.
  - *Reasonableness of precautions:* Absent evidence that Rhino or its counsel took precautions to prevent production of privileged materials, court determined it had "no basis" to conclude any precautions had been taken, let alone reasonable ones.
  - *Time to rectify:* Rhino and its counsel realized they were disclosing privileged material at the time of its production. Thus, Rhino was "chargeable" with five years of delay in rectifying the error.
  - *Extent of disclosures:* While Rhino's original indication that as much as 5% of its production was privileged was later reduced to just 260 documents, court found "this is still a significant number of documents."
  - *Overarching Fairness:* Court determined there was "no fairness" in precluding SEC from using the documents produced by Rhino's counsel, but declined to extend waiver beyond those actually produced.

2009 Annual Meeting  
October 18-21 Boston

*Don't just survive. Thrive!*

---

---

---

---

---

---

---

---

---

---

---

---

**ACC** Association of Corporate Counsel

**AHF Community Development v. City of Dallas, 2009 WL 348190 (N.D. Tex., Feb. 12, 2009).**

- AHF moved for determination that City waived privilege as to emails inadvertently included on disc produced due to conversion to new litigation management software.
- While not specifically addressing FRE 502, court applied factors in *Alldread v. City of Grenada*, 988 F.2d 1425 (5th Cir.1993) to find that privilege was voluntarily waived.
- Emails clearly labeled as attorney-client privileged were marked as exhibits, shown to a witness at deposition, and the subject of substantive questioning – all without objection.

2009 Annual Meeting  
October 18-21 Boston

Don't just survive. Thrive!

---

---

---

---

---

---

---

---

---

---

---

---

**ACC** Association of Corporate Counsel

**Sitterson v. Evergreen School Dist., 196 P.3d 735 (Wash. Ct. App. 2008).**

- Adopted "balanced approach" in *Alldread* to determine whether inadvertent disclosures waived attorney-client privilege as "taking into account both the principles underlying the attorney-client privilege and the realities of modern litigation."
- Application of *Alldread* factors lead to conclusion that School District waived its privilege as to the four documents at issue:
  - No evidence offered of any precautions taken to prevent disclosure
  - District did not notice or attempt to remedy error until three years after it was made
  - 439 documents was not an "enormous" quantity of documents that would excuse an inadvertent production
  - Issue of fairness favored neither party, as the District clearly slept on its rights to object to the disclosure and Sitterson used the documents only to discredit defense counsel at trial

2009 Annual Meeting  
October 18-21 Boston

Don't just survive. Thrive!

---

---

---

---

---

---

---

---

---

---

---

---

**ACC** Association of Corporate Counsel

**Koch Foods of Alabama, LLC v. General Electric Capital Corp., 2008 WL 5264672 (11<sup>th</sup> Cir., Dec. 18, 2008).**

- Affirmed district court's conclusion that Alabama would likely adopt 5-factor "totality-of-the-circumstances test" in *Alldread* for assessing inadvertent waivers.
- No waiver found where:
  - Privileged e-mail was found tucked in middle of 37-page lease agreement contained in a 3,758 page production
  - Document was included in Koch's privilege log
  - Koch immediately objected and asserted privilege when document presented at deposition of its CFO

2009 Annual Meeting  
October 18-21 Boston

Don't just survive. Thrive!

---

---

---

---

---

---

---

---

---

---

---

---

ACC Association of Corporate Counsel

Strategy for Disparate Case Law

2009 Annual Meeting  
October 18-21 Boston

Don't just survive. Thrive!

---

---

---

---

---

---

---

---

ACC Association of Corporate Counsel

502(d) Language

**(d) CONTROLLING EFFECT OF A COURT ORDER.—  
Federal court may order that the privilege or protection is not waived by disclosure connected with the litigation pending before the court—in which event the disclosure is also not a waiver in any other Federal or State proceeding**

2009 Annual Meeting  
October 18-21 Boston

Don't just survive. Thrive!

---

---

---

---

---

---

---

---

ACC Association of Corporate Counsel

Protective Order Provisions

Pursuant to Rule 502 of the Federal Rules of Evidence, the inadvertent disclosure of protected communications or information shall not constitute a waiver of any privilege or other protection (including work product) if the Producing Party took reasonable steps to prevent disclosure and also took reasonable steps to rectify the error in the event of an inadvertent disclosure. **The Producing Party will be deemed to have taken reasonable steps to prevent communications or information from inadvertent disclosure if that party utilized either attorney screening, keyword search term screening, advanced analytical software applications and/or linguistic tools in screening for privilege, work product or other protection.**

2009 Annual Meeting  
October 18-21 Boston

Don't just survive. Thrive!

---

---

---

---

---

---

---

---

**ACC** Association of Corporate Counsel

### Protective Order Provisions

In the event of the inadvertent disclosure of protected materials, the Producing Party shall be **deemed to have taken reasonable steps to rectify the error of the disclosure if, within thirty (30) days from the date that the inadvertent disclosure was discovered or brought to the attention of the producing party, the Producing Party notifies the Receiving Party of the inadvertent disclosure and instructs the Receiving Party to promptly sequester, return, delete, or destroy all copies of the inadvertently produced communications or information (including any and all work product containing such communications or information).** Upon receiving such a request from the Producing Party, the Receiving Party shall promptly sequester, return, delete, or destroy all copies of such inadvertently produced communications or information (including any and all work product containing such communications or information), and shall make no further use of such communications or information (or work product containing such communications or information). Nothing herein shall prevent the Receiving Party from challenging the propriety of the attorney-client, work product or other designation of protection.

October 18-21 Boston *Don't just survive. Thrive!*

---

---

---

---

---

---

---

---

**ACC** Association of Corporate Counsel

### Protective Order Provisions

Within 60 days of the production of documents, the parties will provide privilege logs for protected materials withheld for attorney-client privilege or pursuant to the work product doctrine (or other privileges or doctrines). The privilege logs shall contain names or e-mail addresses extracted from the topmost e-mail message or hard copy document (To, From, CC, BCC), the date of the topmost e-mail or document, and the basis for the assertion of a privilege or other protection. The Producing Party shall provide a privilege log for all withheld e-mail or hard-copy documents or other materials [including redacted materials]. The Producing Party shall produce e-mail chains and strings, and shall only redact only those portions of the e-mail chain that are protected, leaving all other materials unredacted. **The Producing Party shall log all protected content in e-mail chains and strings by logging the topmost e-mail of the e-mail chain or string, as well as sufficient information regarding the redacted material to allow the Receiving Party and the Court to make a cogent evaluation of the appropriateness of the assertion of a privilege or other protection. The Producing Party shall create a single log entry for each e-mail chain or string. A Producing Party's logging of the topmost e-mail shall be deemed to assert protection for all of the protected material in an e-mail string or chain, including multiple redactions or multiple segments.**

2009 Annual Meeting  
October 18-21 Boston *Don't just survive. Thrive!*

---

---

---

---

---

---

---

---





**White Paper**

# **Is There A Return on Investment for E-mail Archiving?**

## ***Part 1: Understanding Factors Impacting ROI***

Contoural, Inc.  
1935 Landings Drive  
Mountain View, CA 94043  
[www.contoural.com](http://www.contoural.com)

**Sponsored by:**



Copyright 2009 Contoural, Inc.

## DRAFT E-mail Archiving ROI

**Abstract**

*In a difficult financial environment organizations are scrutinizing IT expenditures. Only those projects with a proven return on investment (ROI) are receiving funding. Those looking at e-mail archiving need to ask if there is an ROI for their company, and how can these cost savings be justified. This white paper series examines the return on investment for e-mail archiving. It examines how organizations evaluate investment in technology and the four critical factors an e-mail archiving ROI should include. It includes some case studies on ROI investment, as well as strategies for building a business case. Any organization considering an e-mail archiving system will need to face these issues. This white paper helps you make sure you are looking at the right things.*

*This is the first white paper in a two-part series. This first white paper addresses:*

- 1. What's So Special About E-mail*
- 2. IT Portfolio and Return on Investment*
- 3. Evaluating Factors Impacting ROI*

*The second white paper in the series addresses:*

- 4. E-mail Archival ROI Case Studies*
- 5. Strategies for Building a Business Case*

**Note:** *Legal information is not legal advice. Contoural provides information pertaining to business, compliance, and litigation trends and issues for educational and planning purposes. Contoural and its consultants do not provide legal advice.*

## DRAFT E-mail Archiving ROI

### Introduction

Today many organizations are asking themselves if they should invest in an e-mail archiving tool. According to Osterman Research, more than 63% of large and midsize organizations will purchase or have purchased an e-mail archiving tool by the end of 2009. While there has been significant publicity around problems companies have faced for their inability to find e-mail, as well as regulatory requirements for saving *some* e-mail messages, what is not clear is if these same factors apply to your company, and whether you can justify purchasing an e-mail archiving solution.

At a time when many organizations are watching expenditures carefully, and being forced to do “more with less,” it is even more important to understand the degree to which your e-discovery, compliance and storage needs can justify the purchase of an e-mail archiving system. Rarely can an e-mail archiving system be justified on a single factor. Companies are well-advised to build a business case based upon a number of factors to justify the investment. The challenge is to create a business case not on what other companies have or will experience, but rather, one that details the likely return on investment for your environment.

### What's So Special About E-mail?

What's so special about e-mail that it needs to be archived, and why now?

E-mail tends to be different than other forms of communication. First, it is a critical application. Ask any CIO which application she would restore first in an outage: the financial system or the e-mail server, and most would start with the e-mail server. Next, there is a lot of e-mail. The average employee sends or receives more than 140 e-mails per day.<sup>1</sup> The volume generated has been steadily increasing for the past ten years. Unless otherwise archived, managed or deleted, an organization can have literally hundreds of thousands or even millions of e-mails, often stored either on expensive file shares in offline “PST” or “NSF” files, or squirreled away in even more difficult-to-reach places.

Another important factor is how the status of e-mail has changed. E-mail grew up “organically” as an informal communication system within IT, and historically has had few of the controls for managing its creation or distribution afforded other media such as paper documents. For many years as it grew, no one took it seriously as a business document; it was not viewed as a “real” record. This has changed in the past ten years as both courts and regulators have recognized e-mail to contain important information.

Regardless of whether you view e-mail as an official business document, the courts and the regulators do. This is greatly impacting areas such as compliance and e-discovery. In a December 2008 survey, 87% of lawyers believed that electronic discovery is too costly and is driving up the cost of litigation.<sup>2</sup> While most e-mails are not considered “business records,” some e-mails do contain records or other important information. Companies are realizing that e-mail does need to be controlled, and failure to do so may have financial and other impacts. Increasingly, organizations are turning to e-mail archiving applications both as a way to save on

## DRAFT E-mail Archiving ROI

disk storage space, and also as a way to control what e-mail they do have, simplifying search, retrieve and automating destruction.

For many organizations these new requirements for controlling e-mail are not new. Rather, while most companies realize that e-mail must be controlled, the key issue they are struggling with is whether the costs and risks of not controlling e-mail justify the purchase of an e-mail archiving system.

### IT Portfolio and Return on Investment

Should your company invest in any e-mail archiving system to keep better control of what you have where? Will these systems save you money and help you avoid costs, or are these expenditures unjustified in these difficult economic times? Our experience in working with many different organizations is that the answer varies. E-mail archiving makes strong financial sense for many companies, and is more difficult to justify for others. Most important, we have found that a “one size fits all” approach does not work when evaluating ROI. Companies need to look at their own, specific factors.

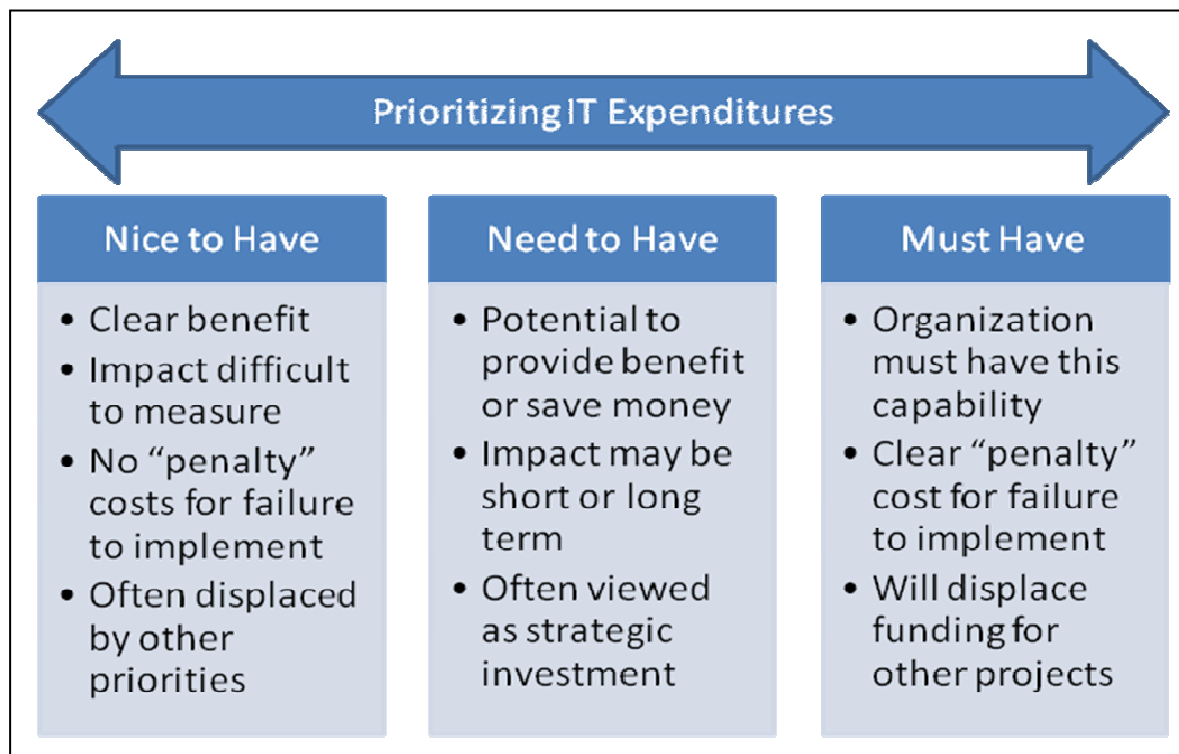
A good way to frame this discussion is to review how organizations invest in technology. Unless providing IT services is a core competence of your company, most view IT investment either as a way to make the business more productive or profitable, or to help reduce costs. With nearly unlimited demand for new functionality and services and very limited resources, CIOs need to spend their budgets wisely. If it cannot be justified under either of these drivers, the company is unlikely to fund the application. Clearly, e-mail archiving has the potential for companies to achieve these benefits, but to what degree? One useful way to answer this question is to map out the benefits on a simple spectrum (see Figure 1.)

When deciding what new applications to purchase, CIOs often classify them into three separate “buckets”:

*Nice to Have* – These are applications that provide value such as increased employee productivity, which in turn may increase an organization's competitiveness, etc. Nevertheless, these “nice to have” benefits tend to be soft; they are difficult to measure in terms of cost savings or increased profitability. These types of projects tend to be the first to be postponed or eliminated when budgets are tightened. Note: many applications can be classified as “Useless to Have” and are excluded from this discussion.

*Need to Have* – Often viewed as “strategic” investments, these are characterized by clear benefits, likely cost savings, improved management. They include a clear return on investment, although often this return is spread over a longer period. Most important, while an organization may miss an opportunity to save money by delaying the purchase of “need to have” applications, they do not face a “penalty” in increased expenses in other areas if they delay deploying. This is missed cost savings. Need to Have funding is more resilient, but when organizations reduce budgets they are often postponed until “next quarter” or “next year”.

## DRAFT E-mail Archiving ROI



**Figure 1 Prioritizing Funding.** During times of restricted funding, organizations typically only invest in "must have" applications.

*Must Have* – Applications classified as “must have” are as the label implies – must have. Companies must deploy these applications, or face highly likely additional cost, penalties, and risks or miss the window for a significant new market. When recognized, companies will always fund “must have” applications, often taking budget dollars from other areas to fund these projects. An important component of “must have” is the implied penalty – “if we don’t buy this now, we will incur other greater expenses.”

Over time, applications can migrate along the “technology adoption lifecycle<sup>3</sup>” and can become more important to an organization, changing from nice to need to must have. An example of this is Enterprise Resource Planning software, such as SAP or Oracle Financials. In the late 1980s this expensive software was viewed as nice to have – a productivity tool for companies to better manage their businesses – but not required. In the early to late 90’s as then current, home-grown accounting applications became more expensive to modify and maintain, these financial packages were viewed as a need-to-have “strategic move” that with an upfront investment could save them money over the long term. Then in the late ‘90s the Y2K issue drove these applications to become must have for many organizations. Unless a company could prove its existing financial package as fully Y2K compliant – capable of handling the new millennium dates – outside auditors would flag this as an unacceptable risk. The auditors were clear: either get a new system or in many

## DRAFT E-mail Archiving ROI

cases companies would fail their audit. Companies faced little choice but to upgrade their systems - clearly "must have".

### Evaluating Factors Impacting Your ROI

In difficult economic environments most companies will only fund "must have" and occasionally "need to have" applications. Even when a potential application can demonstrate a clear ROI, many companies defer nice or many need to have applications for later. It is not that many of these applications do not provide value – many do. The real issue is whether they provide enough value to displace acquisition of other, less value-providing applications. In terms of investing in an e-mail archiving system, the question is often not around the importance of saving e-mail. Rather, the question is whether current capabilities for retaining e-mail will suffice, or whether an organization incurs additional and greater costs and potential penalties through existing processes instead of investing in an e-mail archiving system.

When evaluating e-mail archiving systems, companies often only evaluate storage cost and mailbox management savings (discussed below) exclusively. We have found that while important, storage cost savings are not the largest factor impacting costs. Put another way, we have found it difficult to build a business case for e-mail archiving based on storage costs alone.

Rather, we have seen most successful ROI analyses are based on four drivers: Litigation and E-Discovery Profile, Regulatory Profile, Storage and Mailbox Management Costs and Employee Productivity and Culture. After incorporating these four factors into the analyses, there is no assurance that you can justify the purchase of an e-mail archiving system. You can be assured, however, that you are looking at the right issues.

#### Factor 1: Litigation and E-Discovery Profile

Unfortunately, nearly all businesses face litigation sometime. Increasingly, discovery of electronically stored information (ESI) is a large component of litigation costs. According to Socha Consulting, e-discovery represents more than 50% of the cost of litigation, or \$2.865B in commercial litigation in 2007. A former New Jersey Assistant Attorney General recently stated that the 50% figure is low, and that instead many companies are seeing e-discovery costs grow to more than 70%. In difficult economic times, litigation tends to be counter-cyclical with the economy. When times get tough, people and companies tend to sue more. Additionally, when sued more in tight times, companies tend to settle more quickly.

Much of the discovery is around e-mail. In the words of one litigator: "We always go after the e-mail first. It invariably has the best information." Driven in part by the December 1, 2006 Amendments to the Federal Rules of Civil Procedures, as well as case law emerging around e-mail discovery, companies have new and increased responsibilities to control e-mail in response to litigation. Some of these responsibilities include:

## DRAFT E-mail Archiving ROI

*Duty to Preserve* – Organizations have the responsibility to preserve all relevant documents, including e-mail, upon reasonable anticipation of litigation. You must save all e-mail that *may* be relevant to litigation when you believe your dispute has the likelihood of ending up in court. Many companies have made the mistake of saving all relevant e-mail only after they receive notice of litigation, and face severe consequences when it is shown they anticipated litigation earlier and failed to implement a litigation hold.

*Ability to Search and Retrieve Quickly* – Saving is one thing; searching through what you have is something else. Companies who have used backup tapes to save e-mail and other ESI often have to turn to expensive, outside e-discovery vendors to search and retrieve relevant documents from these tapes. At \$2,000 per tape and higher, discovery costs can quickly balloon into the hundreds of thousands of dollars or even higher. Even if you do not hire outside e-discovery vendors, how much staff time will be spent fulfilling e-discovery requests?

*Cost of Review and Production* – We have found that while most companies preserve enough information, many face the opposite problem – saving too much. Uncontrolled, e-mail over time tends to accumulate. In the event of litigation, a company's identification, preservation and collection of ESI has produced thousands of documents that *may* be relevant. These are often handed to an outside law firm who charges upwards of \$200 per hour to have attorneys review what they have to determine if it is relevant. This lack of control – keeping too much – may have a significant cost impact to companies.

E-mail archiving can have a double-edged impact on the cost of review and production. On one hand, companies with automated archiving systems may indeed save more e-mail which later has to be reviewed. On the other hand, a good archiving system not only enforces collection, it also automates deletion. In some cases, an archiving system can help reduce the quantity of e-mail that is identified for review.

*Ability to Release Holds* – Another significant, often hidden cost of e-discovery is a company's ability to release litigation holds. Once a company has reviewed all e-mail and ESI relevant to a particular matter is brought to conclusion, the company should "release" the hold for all the e-mail and other documents, and as long as there is no anticipation of future litigation. Upon release of the litigation hold, companies can resume their

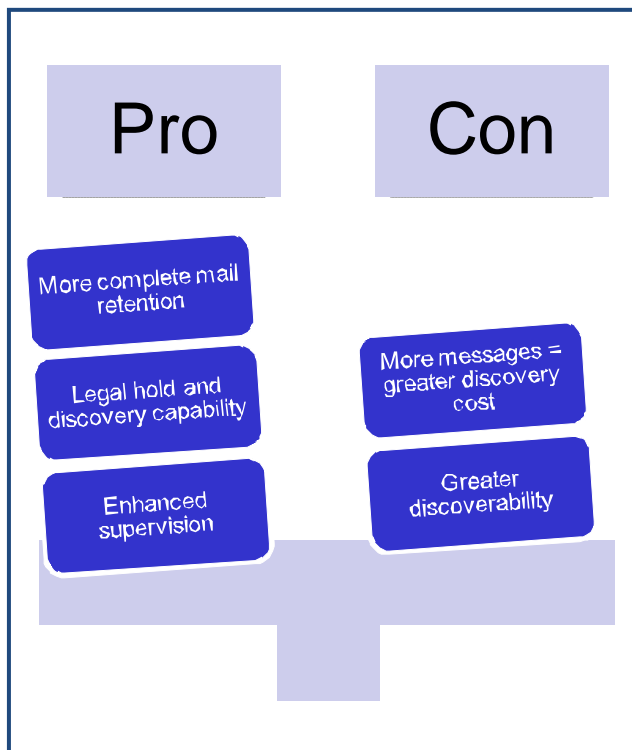


Figure 2. Impact of Archiving in Legal

## DRAFT E-mail Archiving ROI

retention and deletion policy, including deleting older, now released e-mails, per the policy. Unfortunately, many companies are not agile at enacting the release of this hold. When new litigation strikes, these documents held for the initial matter, may be subject to review and production. In not deleting when they could have, additional review of these older documents could represent a huge increase in e-discovery costs.

What is the likelihood these events will impact your company? Clearly there is no predicting with certainty future litigation. However, we have seen some common factors that can be used in evaluating ROI:

*Litigation Profile:* Companies need to ask themselves the following questions: Historically, how much litigation does your organization face? How many matters (cases) does your firm either prosecute or defend every year? Note: while statistics vary, the typical Fortune 500 has more than 150 matters at any given time. How much of your e-discovery was focused on e-mail, specifically? How much did your company pay in e-discovery costs during the past year including internal costs, outside e-discovery vendors and law firms? Have you had to settle any cases because the settlement was less expensive than the anticipated e-discovery costs? Is there new litigation looming on the horizon? How consistent has your litigation profile been from year to year?

*Type of Litigation:* More important than the quantity of litigation is the type of litigation. Organizations should examine the following: What type of litigation does your organization face and by whom? How much of your caseload is employment-related, consumer, intellectual property, and/or class action? Are most of your costs for smaller cases or larger? Do you expect any shift in the type of litigation during the next year, and how will this impact costs?

*Ease or Difficulty of Document Discovery:* When document discovery is required, how easy or difficult is this process? How much time is spent by Legal and IT in responding? How often do you use outside e-discovery vendors? Are there any local e-discovery protocols where your cases are typically tried?

*Litigation Trends in Your Industry:* Are you in an industry that has clearly identifiable trends in litigation? These may include asbestos, banking and financial services, health care, etc. What litigation are your competitors facing, and are there any "cottage" class action plaintiffs active in your industry? How sophisticated in addressing e-discovery are the judges in your common venues?

These issues around litigation are both important and difficult. Sometimes in-house counsel is reluctant to discuss and especially document litigation trends within the company. Sometimes forecasting litigation can be notoriously difficult. Many times, in-house counsel only knows and practices "reactive" e-discovery, and does not realize there may be a better mechanism for controlling e-mail through a proactive archival system.

Nevertheless, litigation and e-discovery are real and ongoing expenses that organizations face, and larger organizations with many different cases can often make a reasonable estimate about future litigation, as least with some types of



## DRAFT E-mail Archiving ROI

cases. Thus we find that if analyzed appropriately, e-discovery and litigation readiness is often the single largest driver for creating an ROI for e-mail archiving. As discussed later, it is important that both Legal and IT collaborate on this analysis.

### **Factor 2: Regulatory Compliance Requirements**

Increasingly, new and existing regulations recognize *some* e-mail as business records that need to be preserved. This is where things get tricky. Currently there are more than 10,000 regulations impacting public and private companies, as well as public sector entities. These regulations require organizations to preserve business records for a specified period of time, and in some instances secure those records. Private companies and public entities sometimes make the claim that as they are not subject to Sarbanes-Oxley (SOX), they need not retain e-mail for regulatory purposes. True, they do not need to save e-mails per SOX, but these private companies and public entities have literally thousands of other regulations that do apply to them and they are required to save some e-mail for these requirements. In many cases, public entities have greater regulatory and statutory requirements than their corporate counterparts.

In developing their record retention schedule around compliance, some organizations make the mistake of classifying e-mail as a particular record type. E-mail is not in itself a record, but rather a medium containing nearly all different types of record and non-record business documents. From a regulatory viewpoint, the challenge is separating the records from non-records. This seemingly easy task is in practice extremely difficult to execute. For some industries, such as the “broker dealer” functions in financial services, classifying records is a clear and prescriptive process. This is the exception. For many other business units, and many other industries, deciding which e-mails contain records and which do not is a complex, subjective, time-consuming, and inconsistent process.

Finally, companies subject to an inquiry from a regulator are required to preserve all relevant documents, not just official records. In many cases, the regulators can demand you produce this information very quickly.

Thus, the business case for e-mail archiving for regulatory compliance focuses around the ability to simplify and automate archiving (often avoiding manual processes and instead implementing role-based archiving), and searching and retrieving e-mail quickly, as well as implementing destruction and audit processes to demonstrate full compliance.

When evaluating their regulatory and compliance risk for retaining e-mails, organizations should consider the following factors:

*Regulatory Environment* – Which regulations is your organization subject to? How prescriptive are these regulations? What are the retention requirements? How quickly must records be produced in the event of a regulatory inquiry? Are there any requirements for saving e-mail on a persistent media, such as “WORM” storage? What type of audit procedures are required to document both retention and deletion of e-mail?

## DRAFT E-mail Archiving ROI

*Amount of Records in E-mail* – What records are contained in e-mail? What individuals' e-mail contains these records? How clearly identifiable are these records within e-mail? How much time would it take for your employees to manually select e-mail for preservation?

*Regulatory Activity in Your Industry* – How active are regulators in your industry? Is there a recent history within your industry of regulatory discovery of e-mail? What are the potential fines for non-compliance?

Nearly all organizations have some e-mail that contains records which need to be preserved. Regulatory compliance is a significant driver in e-mail archiving ROI, especially when compared against the very low compliance and risks of manual processes. However, be careful in building a business case exclusively around compliance. The non-prescriptive nature of many regulations tends to lead compliance-exclusive policies down a rat hole. Rather, this driver is more relevant when combined with other drivers.

### **Factor 3: Mailbox Management and Storage Impact**

Left unmanaged, e-mail tends to accumulate, slowing down e-mail servers and consuming disk space. An e-mail server relatively full of messages within the server runs more slowly, takes longer to recover when restarted, and is more likely to need to be upgraded. Organizations often attempt to address this by imposing mailbox "quotas," limiting the amount of e-mail any single user can store in the server. This of course drives users to store e-mail messages outside of the e-mail server in "PST" (for Exchange) or "NSF" (for Notes) files. These PST or NSF files reside on desktops, file shares, and many other places taking up disk space. There is no assurance that the storage that these files reside on is any less expensive than the storage used by the e-mail server, and we have seen many cases where the storage holding PST/NSF files is significantly more expensive. In one case we are aware of, imposition of mailbox quotas drove everyone to save e-mail on a separate file server twice the cost of the storage used by the e-mail server.

The other approach many organizations take is to implement auto-deletion programs that delete e-mails after 30 or 60 days. These auto-deletion programs do not work, and typically drive "underground archival." (See Case Study in next section.)

## DRAFT E-mail Archiving ROI

In addition to centralizing the storage of e-mail, archiving systems offer an additional benefit that reduces storage. While e-mail messages consume disk space, it is not actually the messages themselves that take up most of the space. Rather, it is the attachments to the e-mail. Within a typical e-mail server, the messages – headers, dates and message text – only consume 4% of the storage space. Attachments to e-mails take up the remaining 96% and are very big compared to messages. In addition to being big, e-mail servers often have multiple copies of the same file sent as an attachment. If someone sends an e-mail with an attachment to five people within a company, the attachment is stored with each e-mail message for a total of five copies in this example.

Most archiving systems take a smarter approach to dealing with attachments, called “single instance store.” Recognizing that an attachment is the same for multiple copies of the same message, a good e-mail archiving system will only store one copy of the

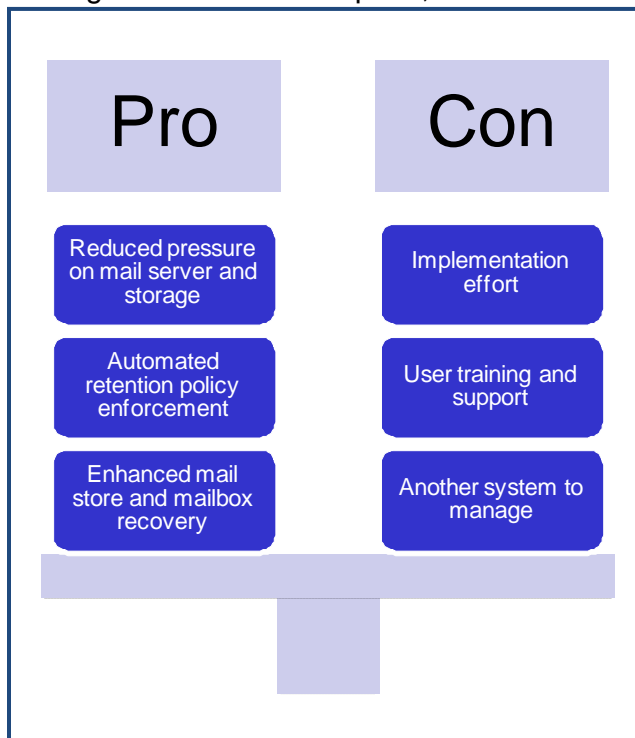
attachment. Each mail recipient thinks she or he has their own copy, while in reality the system has only one. The result is the e-mail archiving system can achieve a “compression” effect, reducing the size of e-mail to be stored by as much as 70%. For organizations with a large amount of e-mail both in their e-mail server as well as in PST files, consolidating all of these messages into a single archive and achieving this “compression” effect significantly reduce the cost of storage.

Will implementing e-mail archiving achieve a suitable ROI for IT for your organization? Here are some of the factors you should consider:

*Number of Mailboxes* – The more mailboxes you have, and the greater the size of each mailbox, the more likely that the reduction of storage cost gain in an e-mail archiving system will help justify the system. Organizations need to look at how much e-mail they have on what types of systems. It is important to include offline PST/NSF files, especially those that reside on expensive file shares.

*Performance and Availability of Mail Server* – A mail server “clogged” with significant online stores of e-mail performs more slowly. If you are considering upgrading your e-mail servers, you may ask if that money is better spent on an e-mail archiving system to achieve the same result.

*Distribution of E-mail Servers and Users* – Companies with users spread across many locations, such as a number of branch offices, may benefit from consolidating multiple e-mail servers into a single system. Likewise, sometimes companies can



**Figure 3. Impact of Archiving on IT**

## DRAFT E-mail Archiving ROI

save by aggregating a number of remote file servers storing e-mail into a single e-mail archive. The cost of managing the archive may be less expensive than managing a large number of small file servers. One additional option is outsourcing e-mail entirely to a hosted provider. E-mail archiving may be an important component of that decision.

*Consolidating E-mail Backup* – Deployment of an e-mail archiving system may reduce the load of the backup server, both through the effective compression of e-mail as well as through the reduction of the number of backup streams.

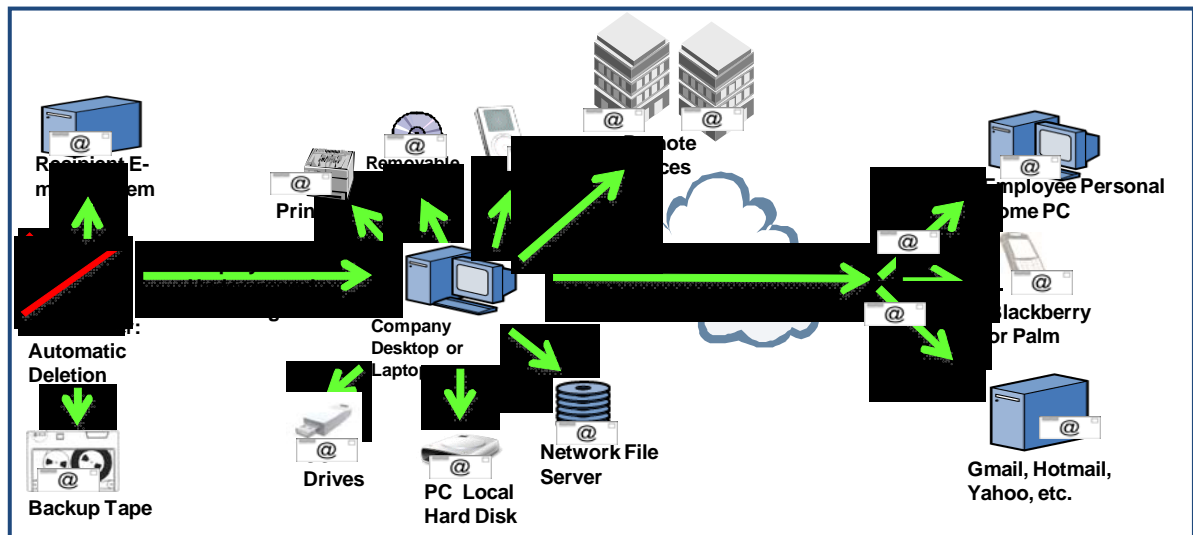
*E-mail Management Operational Costs* – Typically the greatest cost in managing an e-mail system is IT staffing. Reducing e-mail management will reduce IT workload and have a direct and measurable cost benefit. In the event e-mail is moved to a hosted provider, this can result in larger cost reduction.

### **Factor 4: Employee Productivity and Culture**

Perhaps one of the most overlooked issues in e-mail archiving is the impact on employee productivity and culture. Good archiving strategies recognize both how employees use e-mail, and the consequences if the company deletes e-mail for which employees require access. In other words, what will employees do regardless of your policy? E-mail is the de facto communication mechanism for most companies. Employees use it so much because it makes them more productive, and in many cases it serves to record many of the decisions. Like it or not, e-mail is not going away soon.

Faced with increased e-discovery, uncertain regulatory requirements and increased storage costs, many companies have adopted either thirty or sixty day e-mail deletion policies. While this works in theory, it fails in practice. We have found that companies that automatically delete e-mail from their system after thirty or sixty days do not actually delete e-mail. Rather, users engage in “underground archiving.” (See figure.) Users print out e-mail, or save it on iPods, copy it USB drives, move it to a PST file or even e-mail it home. Deletion strategies don't delete. Instead they spread e-mail out all across the enterprise, in the nooks and crannies of the IT infrastructure. This simply makes it more difficult and expensive to discover when you need it.

## DRAFT E-mail Archiving ROI



**Figure 4. Thirty or sixty day e-mail deletion policies drive users to "underground archiving."**

How do you factor these issues into ROI?

*Understand Productivity Impact* – While difficult to measure, e-mail is an employee productivity tool. How much time can employees save if e-mail is more productive?

*Gauge Cost of Manual Archiving Process* – Often the alternative to an e-mail archiving system is to have employees manually save relevant messages to a special archive folder. With the average employee sending and receiving more than 140 messages per day, this process of selecting and classifying all messages done correctly can require upwards of an hour per week per employee. Any ROI evaluating a manual archive should include time employees spend each week doing this. For larger organizations, this cost can grow quite large.

*Cost of Underground Archiving* – The ROI should incorporate the cost of underground archiving practices against an e-mail archive. This is typically reflected in increased discovery costs, as well as additional disk usage.

## Conclusion

In budget-constrained spending environments, organizations typically will only fund “must-have” projects. Developing a must-have ROI for e-mail archiving requires not only examining savings in storage costs, but more importantly, reviewing the e-discovery, compliance and employee productivity impacts. Only then is there likely to be enough of a justification.

## DRAFT E-mail Archiving ROI

<sup>1</sup> Osterman Research, Inc. Messaging Archiving Market Trends, 2006-2009

<sup>2</sup> Joint study sponsored by the American College of Trial Lawyers and Advancement of the American Legal System, December 2008.

<sup>3</sup> See *Crossing the Chasm: Marketing and Selling High-Tech Products to Mainstream Customers* (1991, revised 1999), Geoffrey A. Moore, Harvard



White Paper

## Legal Aid: How IT Can Be the Difference Between Litigating or Settling

Understanding which responsive electronic records are accessible and relevant can make all the difference early on when assessing a legal case. Often, IT finds out too late that it should have been saving certain data or is asked to quickly locate responsive records based on vague or incomplete descriptions. Map your electronic information stores ahead of time and proactively index your data sources so you will be prepared when the General Counsel comes knocking!

Sponsored by StoredIQ

How IT Can Be the Difference Between Litigating or Settling

**Table of Contents**

Introduction..... 3

ESI: E-Discovery Under Pressure..... 3

Locating and Mapping Data..... 6

Understanding Data Topology..... 7

Advanced Content Analysis..... 8

Conclusion: Early Assessment..... 8

About Contoural, Inc. .... 10

About StoredIQ, Inc..... 11



## How IT Can Be the Difference Between Litigating or Settling

### Introduction

Litigation is one of the nightmares that IT staff fear most: How do we respond when the General Counsel comes looking for electronic records we didn't even know we had? What happens when the fate of the company rests on producing a few old email messages or files sitting on the network or a remote server?

IT is used to working under pressure. Putting forth best efforts doing the best job possible with limited resources and technology; however, "best effort" work is not sufficient when it comes to preservation of evidence for litigation. The *time* required searching through terabytes and terabytes of data on a multitude of systems can put a legal case in jeopardy in and of itself. IT systems are just not created with legal requirements in mind – they are designed for end-user performance and availability, not preservation, distributed search, culling and legal production.

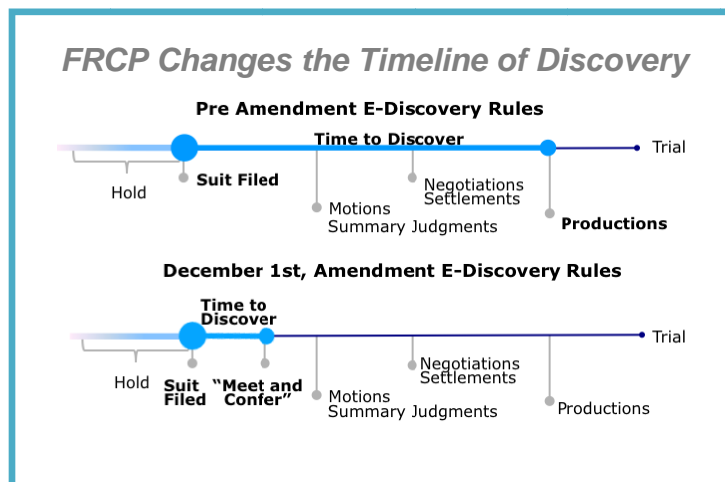
Good news – help is at hand. A new partnership is being forged between the legal and IT departments at many organizations. The focus is on electronically-stored information (ESI), with records management joining the discussion. IT systems and tools are evolving as well, enhancing litigation capabilities but also delivering value for information lifecycle management and capacity control. When it comes to production of records for legal cases, IT is being transformed from a technical roadblock to a risk and cost-mitigation powerhouse!

*IT systems and tools are evolving, enhancing litigation capabilities and delivering value for information lifecycle management and capacity control. When it comes to production of records for legal cases, IT is being transformed from a technical roadblock to a risk- and cost-mitigation powerhouse!*

### ESI: E-Discovery Under Pressure

Legal cases have always turned based on the evidence available, but the law is only recently adapting to the new world of electronic records. Just a few years ago, it was common for legal counsel to request printouts of information stored within electronic data systems; however, the transformation of business communication through the use of email has changed all that. Today, as nearly all discovery requests ask for email and native files, ESI has become the single most important source of evidence before the court.

One major challenge to the status quo of legal discovery is the amendments made at the end of 2006 to the Federal Rules of Civil Procedure (FRCP). The FRCP apply to any company or organization involved in litigation in the United States Federal Court system. It has undergone a multi-phased



## How IT Can Be the Difference Between Litigating or Settling

evolution. Electronic records were first recognized as admissible documents in the 1970s, but the December 2006 amendments represent a sweeping change to how electronic records are handled in litigation and investigations. The recent codification formalized the definition of Electronically Stored Information (ESI), specified its discoverability, and laid out the duty of organizations to preserve ESI when litigation is pending or “reasonably anticipated.” Other key elements include new mandates for initial

disclosure of data in a party’s control that it may use to support its claims or defenses<sup>1</sup>; a requirement for both parties to “meet-and-confer” early in the case to develop a proposed discovery plan<sup>2</sup>; allows the requesting party to specify the format of the data to be produced; requires that the responding party produce an ESI resource map or topology containing potentially responsive information that was not searched or produced; allows some cost shifting for “inaccessible” information; and, creates the provision that “Safe Harbor” is offered for protection from spoliation sanctions as a result of regular data management operations based on an established records management plan<sup>3</sup>.

Recognizing that electronic data and other forces of modern business were radically changing

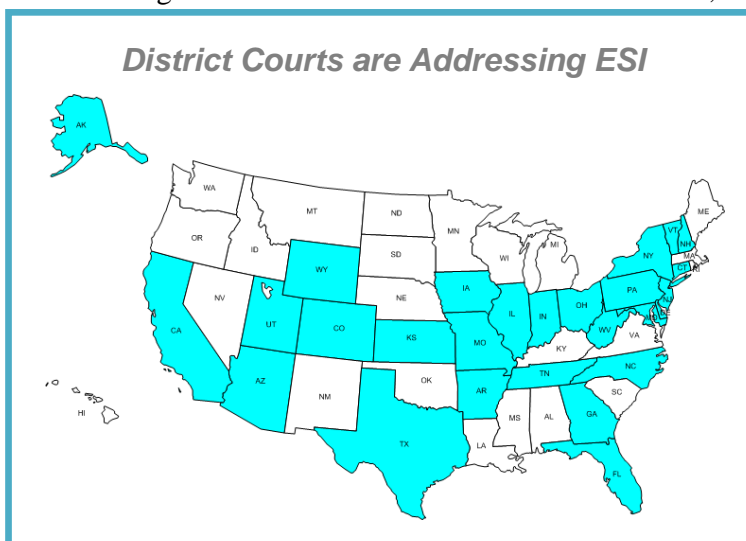
### *What Should Be Included in an ESI Map?*

The ESI map should include all electronic information held by an organization, including:

- Applications like email, file servers, web servers, document management systems, and enterprise applications
- Business applications like financials, budgets, HR, process control
- Infrastructure like backup servers and tapes, firewalls, and authentication systems
- End-user device data on laptops, desktops, PDA's, phones, and portable drives

the legal landscape, leading experts in the legal community began meeting in Sedona, Arizona to advance the law. Their annual conferences have produced a wealth of information in a variety of fields, including the retention and production of electronically-stored information or ESI<sup>4</sup>.

Among the best practices espoused by these and other



<sup>1</sup> FRCP Rule 26(a)(1)(B)

<sup>2</sup> FRCP Rule 26(f)

<sup>3</sup> FRCP Rule 37(f)

<sup>4</sup> For more information on The Sedona Conference, including publications devoted to best practices and commentary on ESI, visit <http://www.thesedonaconference.org>

## How IT Can Be the Difference Between Litigating or Settling

legal experts is preparation for electronic discovery by creating a topology or data resource map of all ESI retained by an organization. This ESI map is a written overview for use by legal counsel when preparing for the “meet-and-confer<sup>5</sup>” process regarding litigation discovery. It lists the likely custodians of relevant electronic materials, the electronic systems and formats that contain them, and any limitations to their accessibility. This map is an internal-facing document, but the data it contains allows the legal team to precisely and confidently discuss which electronic records they have and whether or not they are reasonably accessible.

The ESI map continues to be of assistance as the case progresses, allowing legal counsel to act quickly and independently as new requests are made. When done properly, each category of ESI is accompanied by a report with an audit log related to the electronic data subject to its topology mapping. The litigation team can go directly to the system containing the map and reports to clarify location, system type, retention policies, scope, and character of each type of record. Although mandated in litigation by the FRCP, ESI maps are also useful for other types of discovery, including regulatory compliance and investigations, and litigation in state courts, many of which have adopted similar ESI requirements.

The concept of the ESI map is new to many lawyers, however, so one should also consider what such a map is not. First, realize that it is not matter-specific – an ESI map should be a general list of all of the ESI within an organization, not a special-purpose document created for a single case. The basic units of information in an ESI map include the data store format, location within the network, storage size, and record type. Generally, it is not an employee-level view of all of the data that one has access to; however, with today’s technology it can be. It is also not an individual listing of all documents, records, or data within an organization but a list of record categories, broken out along lines that would be relevant to the legal audience that will make use of it. The creation of the ESI map is also not the time to pass judgment or give opinions as to the relevance of individual documents – list everything and let the legal team decide what is useful and what is not.

Many companies today have already put together ESI maps, and they are finding them to be very useful. Even in the absence of litigation, the creation of a map is an opportunity to consider and address the records management processes in place, as well as to improve the available options for preservation of records. Once litigation seems likely, the map allows the legal team to accelerate the discovery of relevant documents and thus have more time to conduct an early case assessment. The map also helps the legal team to construct arguments regarding the relative accessibility of various data types. Most importantly, the map allows the legal team to set a confident tone of defensibility during the Rule 26(f) “meet-and-confer” sessions with opposing counsel.

---

<sup>5</sup> FRCP Rule 26(f)

## How IT Can Be the Difference Between Litigating or Settling

### Locating and Mapping Data

Since the map contains a record of all locations and types of electronic information in an organization, building an ESI map manually can be a time-consuming process. Many have created their maps through exhaustive interviews with representatives from all parts of an organization. Others have attempted to create dynamic maps through the use of homegrown or third-party software applications. Finally, many have tried a hybrid approach, merging interview data with output from applications and lists of data types. With the latest technology in today's marketplace, the manual ESI map building should be a thing of the past.

Static ESI maps, created by hand, are most appropriate for smaller organizations or those with narrow, focused businesses. For example, a company with a single focus or product, where the majority of employees interact with a similar set of data, are able to limit the number of interviews and involved parties and can create their maps with relative ease. Very small organizations face a similarly simple task, as an exhaustive interview schedule will not require many participants. Larger organizations can create static ESI maps if they are willing to devote enough time to the creation, or if an outside party can be brought in to do the work. Regardless of the creation process, however, manual maps are, by definition, static and will require updates over time and are fraught with peril from a legal risk standpoint.

Information technologists often look on the difficulty in creating an ESI map as a solvable computational problem: They believe that the creation of a dynamic map is a challenge they are up to facing. Beware, except in the simplest of circumstances, homegrown ESI mapping applications have proven challenging to create and defend in court. Therefore, larger companies with more mature and varied infrastructure should rely on specialized mapping applications if they wish to create a dynamic map. These applications integrate various data feeds from HR, asset management, storage resource management, IT repositories, and all the other systems in a corporate network into a unified record in a database, portal, or similar application. The variety of information data sources can prove challenging, and the needs of an ESI map are different from typical standalone application management challenges.

Therefore, special-purpose ESI mapping software is the key to creating a usable, repeatable and defensible dynamic map.

Most organizations that rely on dynamic mapping technology actually use a hybrid approach, combining objective data from their dynamic ESI application with subjective commentary and input from personnel. In this case, the ultimate ESI map is not the output of their mapping application but a second portal, database, or

#### *Key Factors in Deciding Between Dynamic and Manual ESI Maps*

The difficulty in creating a map must be balanced against the risk that it does not reflect the reality of a dynamic set of electronic systems. Consider the following factors when deciding whether to manually create your ESI map or use specialized mapping software:

- Current and forecasted litigation profile
- Industry
- Size of organization and number of employees
- Regulatory requirements
- Amount and distribution of ESI
- Anticipated venues
- Ability to maintain over time
- Willingness to invest now to avert future cost and risk

## How IT Can Be the Difference Between Litigating or Settling

interface which uses the dynamic application as a reference but correlates it with manual inputs.

## Understanding Data Topology

Regardless of whether a manual or dynamic map is needed, the first step is comprehension of the “lay of the land” for data storage. Although the majority of business-critical applications naturally reside on centralized servers, critical data can often be found in many locations. It is paramount that IT staff develop an overview to understand the scope of the mapping task.

A data topology assessment begins with an overview of the various locations where data can reside. How many files, messages, or other objects are found? What is the total amount of data? These questions can help to prioritize further assessment efforts, and can also be useful in legal discussions later on. A file server with thousands or millions of files would obviously be very difficult to place under legal hold, assess and review, and discuss in court!

One often-overlooked factor is duplication of data. While initial preservation requirements call for a big net over everything responsive, there ultimately is no need to retain, search, and produce every copy of a file. Fortunately, many tools exist to digitally hash and compare files to determine whether they are exact duplicates. This can become challenging at scale, however, once large numbers of files are involved and with duplicates residing in many different locations. Another challenge is examining near-duplicate files. Specialty software is required to perform this type of analysis.

Another key consideration for understanding the topology of stored data is the age of data. Legal cases normally focus on data within a well-defined range of dates, but even those that are more flexible in their searches normally have rough date ranges. A case involving a specific event would normally not hinge on data produced well before or after that date, for example. Understanding and implementing a data topology solution can also expose weaknesses in corporate record retention execution. If record retention policies are not enforced, the volume of records to be produced in legal cases will grow.

A helpful bit of topology information relates to the meta-data or type of records stored in a given location. Computer systems generally classify files based on the application that created or makes use of them, and this information helps understand their content. For example, Microsoft Excel spreadsheets would likely contain numerical analysis, while graphics files would be more relevant to creative departments. Many files contain various types of data. A Microsoft Word or PowerPoint document might contain spreadsheet data and illustrations in addition to text. Email messages also often contain attached files of various sorts, making it difficult to classify them.

Most data storage systems also record an owner and group for each file or message, and this can be helpful as well. Legal hold and discovery often includes a list of individuals or departments of interest, and meta-data is helpful to focus efforts for location, assessment and preservation of data.

One important fact when considering meta-data is that it is not always reliable if not preserved properly. It is trivial to change the owner or date associated with a file stored on most common file systems. Even the file type can be disguised by changing the name or other metadata. And many computer systems routinely package and compress multiple files in generic archives (e.g. zip, tar, and pst), which can interfere with assessment and reporting.

## How IT Can Be the Difference Between Litigating or Settling

Despite these limitations, a solid report of data topology can prove useful before and during legal actions. Consider, for example, a case involving employee performance and compensation. The data topology map would quickly eliminate data relevant to other departments and stored on servers that the employee did not have access to. Since this data would be less likely to be obfuscated, intentionally or accidentally, the file type and ownership meta-data would be useful to hone down the list of records to be held and turned over to counsel. In addition, retention server platforms that utilize WORM-based storage can be leveraged to preserve meta-data to protect against accidental or malicious modifications.

## Advanced Content Analysis

As discussed above, basic system meta-data is often too generic to be used for much more than a basic overview, and can be unreliable as well. To address this issue, some specialized software exists that can look inside files and build searchable indexes. These applications are much more difficult to fool, since they examine the actual data contained in a record.

One very promising development is the creation of a set of common data types that can be detected within files. Since many common elements contain recognizable patterns, software can detect and index them. Credit card, social security, and phone numbers, for example, conform to strict formats and are relatively simple to identify. Addresses, place names, organizations, and other textual data are more flexible, but advanced systems can still pull these out of files for later use. Finally, there is a class of more specific vertical data types, such as business or medical terms, which can prove very useful but are much more difficult to identify as they typically require domain expertise to recognize and classify properly.

Systems that perform this kind of advanced content analysis can be tremendously useful in ESI mapping, early case assessments, preparing for legal holds, and discovering records for legal counsel. Content-based meta-data is much more reliable than generic system meta-data since it is both more thorough and much more difficult to hide. With content analysis, re-named file types can be quickly discovered. Even archives like .zip or .pst files can be examined in this way to identify their true contents. Encryption, however, can still hide data from this type of analysis, since these systems can only index the records to which they have access.

Queries using advanced content analysis are also much more straightforward and understandable for non-technical audiences. Rather than searching for an Active Directory ID, they can specify the name of an employee, for example. And legal counsel will be much less frustrated with overwhelming numbers of potential matches when searching for credit card numbers or health plan beneficiary numbers, since these tools validate the data as they search.

## Conclusion: Early Assessment

Legal action rests on evidence: Whoever gets their hands around the facts the quickest has the advantage. Whether a case is won or lost is often reflected in the electronic documents discovered. The upshot of the creation of an ESI map combined with the use of an advanced content analysis tool is the ability to provide reliable information to legal counsel in a timely manner. A data map alone, without additional insight and knowledge about the content of the data, will not yield a complete and accurate picture of what electronic data an organization possesses and the potential risk and relevance of such content. Without this

## How IT Can Be the Difference Between Litigating or Settling

level of intelligence, a responding party will be at a disadvantage when it comes to making early strategic decisions regarding litigation matters and investigations. This can lead to costly mistakes in terms of time, money, and public reputation.

As illustrated above, the legal team has only a few weeks to assess the potentially discoverable electronically-stored information before meeting with opposing counsel. If they can feel confident that they know the true scope of ESI within the organization, thanks to the ESI map, and can interactively query these records, thanks to the analysis tool, they will be much more confident in their ability to respond.

ESI maps help the legal group in many ways. An ESI map helps legal counsel prepare for the Rule 26(f) “meet-and-confer” session’s discussions of accessibility, production format, and cost shifting. It helps the legal staff understand the extent to which data is accessible, based on the burden and cost of accessing it. If certain records are especially difficult to access, the organization may be able to shift the cost of production to the opposing party. The ESI map combined with thorough content analysis capabilities also reduces the time required to prepare for the meet-and-confer” session, reducing legal fees and the cost of liability insurance. Knowledge of relevant facts, keywords, and custodians prior to meeting with opposing counsel provides a strategic advantage when negotiating criteria for legal discovery of electronic content. A good map can be reused in subsequent matters and can improve records management, legal hold, and preservation efforts.

IT benefits from the creation of an ESI map as well. They can avoid the time-consuming last minute “fire drills” that happen when legal action becomes likely. The map also reduces the load from regular legal hold and e-discovery requests since litigation will follow the map, going directly to the assigned system owners and answering their questions on scope and format of data in a self-service fashion. The creation of the ESI map is also an excellent motivator to create the application and data inventories so often desired but so rarely created, and may provide the financial backing for infrastructure upgrades through litigation cost savings.

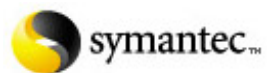
*Note: Legal information is not legal advice. Contoural provides information pertaining to business, compliance, and litigation trends and issues for educational and planning purposes. Contoural and its consultants do not provide legal advice. Readers should consult with competent legal counsel*



White Paper

# How Long Should Email Be Saved?

Sponsored by Symantec, Inc.





How Long Should Email Be Saved?

## Table of Contents

Introduction.....	3
Considering Email retention .....	3
Can IT Set Email Retention Policy? .....	4
Best Practices .....	4
What Does An Email Retention Policy Look Like? .....	5
Determining Email Retention Periods: Keep it Simple.....	5
General Business Correspondence .....	6
Functional Departments, Titles or Names .....	6
Managing Exceptions .....	6
Regulatory Compliance Requirements .....	6
What Are The Key Elements Of An Effective Records Retention Program? .....	8
Create a Core Team.....	8
Assessment .....	8
Record Retention Policy and Schedule .....	8
Solution Implementation Planning.....	9
Education and Training .....	9
Audit.....	9
Implementing Your New Policies.....	9
Getting Help .....	9
Using Enterprise Vault .....	10
Conclusion .....	10
About Contoural, Inc. ....	12
About Symantec Enterprise Vault .....	13

## How Long Should Email Be Saved?

*Note: Legal information is not legal advice. Contoural provides information pertaining to business, compliance, and litigation trends and issues for educational and planning purposes. Contoural and its consultants do not provide legal advice. Readers should consult with competent legal counsel.*

## Introduction

As email has become more critical in the business world, many companies are weighing the question of how long it should be retained, what should be done with it, and when it should be deleted. The answer depends on many issues, particularly when one considers the varying regulations and business situations that might demand emails to be archived for long periods of time. This white paper examines the reality of records retention and email archiving, focusing on the process of developing an effective retention policy and automating solutions to enforce rules and satisfy retention obligations. Contoural will also recommend best practices for email retention and real world examples.

## Considering Email retention

As many high-profile cases have shown, failure to comply with an e-discovery request for e-mail as part of the litigation process can have a tremendous impact on businesses. Numerous internal policies and external regulations call for long-term retention and preservation of email, and many business circumstances demand recovery of historic messages as well. To ensure organizations will be able to meet these twin demands of litigation and legislation, all organizations, from the smallest private companies to the largest government agencies, must create a policy regarding long-term storage and handling of email messages.

Recent studies show that nearly half of all companies have some policy for email retention, but less than one in eight has implemented an automated solution to ensure requirements are met. Having an un-enforced policy is the worst possible scenario. Organizations can be held legally liable if their policies are not strictly followed, and only an automated system can help ensure compliance.

Email is a special, and critical, example of an application that, by default, lacks retention enforcement. Modern email systems are designed to be the hub of high-volume, daily communication. Applying record retention periods usually requires the addition of a third-party application. Relying on users to manually apply corporate retention policies is not only naïve but technically impractical.

### *Manual vs. Automatic*

When considering e-mail message retention, IT organizations have a key decision to make:

*Should users manually classify messages?*

*or*

*Should an attempt to be made to automate this task?*

Manual classification is simpler to implement, but difficult to get right. As users decide which messages to keep and how to classify them, inconsistencies are bound to spring up, and productivity is lost. Automation can ensure consistent classification, but it is difficult to create a system that recognizes the nuances of business communication. An ideal system would combine the best of both worlds, automating simple tasks and requesting user input for more complex decisions.

## How Long Should Email Be Saved?

The daily volume of email entering and exiting each user's mailbox, multiplied across the entire enterprise, necessitates an automated solution to enforce policy.

Email has other unique aspects as well. Although email has more structured metadata than most corporate applications in the form of headers, some content lacks standards. Subject lines, or even addresses, cannot be relied upon to be specific, consistent, or unique. The proliferation of email attachments creates another unique challenge, with encoded files frequently retransmitted and often containing key contextual information. Ironically, the flexibility of email as a communication mechanism undermines its inherent structure.

Over the last few years, email has also become the primary target for discovery requests during business related litigation. Here again, the flexibility and democratic nature of e-mail communication works against the needs of corporate counsel. In the event of a legal hold request, all relevant files and emails must be immediately preserved, and most e-mail software is incapable of this type of retention. Litigation hold is a joint responsibility of both the IT staff and the legal department, so it clear process must be put in place to communicate hold requirements. This communication must include information about the date and scope of the request, which locations and employees are covered, and the specific records or content that must be retained. Since legal actions can sometimes drag on, IT must also consider how it would handle continued retention for a long period of time.

## Can IT Set Email Retention Policy?

Although IT organizations have proven adept at creating and managing complex technical systems, the creation of business policies has often proven troublesome. Indeed, it is unrealistic to expect the technical organization to create business policy in isolation. Instead, a consensus must be developed with a wide range of opinions throughout the organization.

Although the final, complete policy for email retention cannot be produced by the IT staff alone, they can produce a workable draft policy grounded in the technical capabilities of e-mail archiving software. Once this draft is circulated, it can be tuned to meet the expectations of the business, and integrated into a wider record retention policy. In general, the input from legal, finance, human resources, and business units will be integrated with the consensus from IT management, storage, and messaging representatives.

## Best Practices

Although policies vary based on business circumstances, some universal best practices can be distilled from the experience of many organizations. The following practices are applicable to most email retention systems:

1. An email archiving policy should be part of an overall records management program, which has its own record retention policies and procedures.
2. The scope of the policy should consider all employees who create, send or receive email messages and attachments.
3. The email archiving policy should refer to IT's Acceptable Use Policy and expand upon the areas specifically related to email use.
4. The policy should state whether users can create PST files to store email messages.
5. Data privacy issues should be addressed. Employees should have no expectation of privacy when using company resources for email and could be subject to discovery proceedings and legal actions.

## How Long Should Email Be Saved?

6. The policy must clearly state how and where email records will be managed, protected and retained.
7. The policy should explain how IT handles exceptions to the retention settings (e.g., some countries will require significantly longer retention periods for certain types of records).
8. Managers and users must be provided with training and support.
9. Compliance with the policy must be mandatory for all employees and include compliance in an internal audit review.
10. Review the policy yearly to ensure compliance with any changes or new regulations.

Taking these best practices taken into account and adding any organization-specific element, a draft email archiving policy can be created by IT as a way to kick-off an overall record retention policy modernization effort.

## What Does An Email Retention Policy Look Like?

The key to creating an effective automated e-mail retention system is to keep the retention policy as simple as possible. Not only does simple approach assist in implementation, it also allows ongoing management and monitoring using common sense rather than complex rules. Therefore, an effective email retention policy should be short, specific, and cover 95% of all message traffic. Any exceptions will be handled manually as needed.

One key question to answer when creating an email retention policy is the length of time that most messages will be retained. In addition to the cost of long term storage, there are risks in retaining data as well as in deleting it. Most companies come to the conclusion that many messages should be retained for a few years for business productivity purposes. Once retention stretches beyond the memory of users, it must be indexed and searchable, which normally means keeping messages online rather than on tape.

### Determining Email Retention Periods: Keep it Simple

Over time, the cost of disk storage continues to decline while the length of time messages are retained climbs. Could email storage costs become irrelevant? For instance, the total size of a large enterprise messaging system from ten years ago was likely to be measured in megabytes while five years of email storage may be measured in the tens of gigabytes. Although these appeared to be large numbers at the time, they are small compared to today's enterprise storage capacity. Assuming the cost per gigabyte of storage continues to decline, one could deduce that all messages should be retained forever.

### *Elements an Email Policy*

An email-retention policy should cover all employees, contractors, and others related to the company who create, send, or receive e-mail messages. It should be clear that, in addition to the message body, attachments and headers, including addresses and hidden information, are also part of the policy.

The email policy must specify the following standards:

- Acceptable use of the email system
- Unacceptable uses of email
- Offline copies of email messages
- Privacy issues and local regulations
- Email management and retention policies
- Responsibilities of the staff
- Auditing and processes for dealing with violations

## How Long Should Email Be Saved?

However, there are risks with long-term retention. As the volume of messages increases, the cost of complying with e-discovery request increases as well. A higher volume of messages combined with more powerful search capabilities, can lead to escalating demands on the IT and the archiving solution. A larger message store could also expose the company to legal entanglements, (i.e., the “smoking gun” email message), that otherwise could have been avoided if messages were routinely deleted. In the end, the risk and cost of long-term retention must be balanced against the desire for a complete archive of email messages.

### General Business Correspondence

As stated earlier, the goal of an email archiving solution is to automate the retention, expiry and classification and retention of 95% of all messages. When creating an email retention policy using an automated solution, group messages with similar retention needs logically such as by function, department or title. Most email messages can be classified as general business correspondence with a suggested default retention period of three- to five- years. This single rule will probably cover the majority of all email messages.

### Functional Departments, Titles or Names

Next, find universal and logical criteria to identify and classify the remaining email messages. Experience has shown that two more key criteria will cover these communications: critical organizational departments, and key individuals. Critical departments typically include finance, which may need a retention period of ten years or longer for tax purposes, as well as human resources and legal staff. Certain key management figures or company officials may need indefinite retention of email messages. Include corporate executives, who may have a fiduciary responsibility to the company, as well as directors and members of corporate governance boards.

### Managing Exceptions

A small percentage of email messages will have to be categorized manually. Employees will need to be trained on how to recognize which messages will be exceptions to the general policy, as well as what their retention period should be. Of particular importance are apparently mundane messages whose attachments or context make them critically important. These will have to be managed manually by those familiar with their content. The retention period for exceptional messages will require some research into the specifics of an organization's business functions, and must be done with an eye toward a larger record retention management program.

## Regulatory Compliance Requirements

A wide variety of regulations and standards apply to record retention, and email can be a vehicle for these records. Different regulations will apply to different departments within every business – human resources may concern themselves with HIPAA, facilities may be concerned with OSHA, and finance may focus on Sarbanes-Oxley. Therefore, it makes sense to target the email archiving solution by department or area of responsibility in order to align it with record retention regulations.

The table below shows many of the regulations that might affect record retention and security requirements. Some affect certain market sectors or corporate constituencies, while others are region-specific or focus on public companies or manufacturers.

## How Long Should Email Be Saved?

Sector-Specific Regulations	Financial Services			Health Services		Life Science	
	SEC Rule17a-4	PATRIOT Act	Basel II	HIPAA	CMIA	21 CFR 11	UK GMP
USA Regulations	Sarbanes-Oxley Act (Enforced by SEC)						
	EEOC						
	OSHA						
	Gramm-Leach-Bliley Act (GLBA)			SB 1386			
UK Regulations	Data Protection Act (UK) and similar laws implementing EU Directives				EU GMP Directive 91/356/EEC-9		
	UK Public Records						

Note that most regulations do not specify the mechanism or schedule of record retention. Instead, they detail the desired outcome, whether that is protecting confidential information or producing critical records on demand. However, some regulations do specify retention periods for certain record types, as illustrated below.

Regulation	Focus	Area	Years of Retention	Note
21 CFR Part 11	Life Sciences	Clinical trials	35	Thirty five years from creation
		Food manufacturing, processing, and packaging	2	Two years after commercial release
		Drug manufacturing, processing, and packaging	3	Three years after commercial release
		Manufacturing of biological products	+5	Five years after the end of manufacturing
HIPAA	Healthcare	Pediatric medical records	<21	Until age 21
		Adult medical records	<+2	Up to two years after a patient's death
		Documentation related to security	6	Six years from date of creation
Sarbanes-Oxley	Public companies	Audit-related records	+7	Seven years after the conclusion of the review
SEC 17a-4	Financial services	Account records	+6	Six years after closing the account
		Financial statements, transaction records, communications	3	Two years easily accessible, three years total
		Member registration and corporate documentation	∞	For the life of the enterprise

Note retentions vary relative to different areas of focus: Some concern the lifespan of individual people, others refer to the beginning or end of a product's development, and others are specific to a document or other record. When they take effect also varies – some start counting at creation while others are “term plus”, adding years after an event. Another

## How Long Should Email Be Saved?

consideration is whether the regulation calls for a positive end or not – some demand an action at a certain time, while others are minimums.

This can get quite confusing. HIPAA, for example, calls for retaining adult medical records only for two years after a patient's death but retaining pediatric records until the patient reaches the age of 21. This means that a retention scheduler would have to have access to birth dates and death records, which would likely be injected come from an outside source. Automating this type of retention schedule can test the flexibility of both the archiving product and the programmer assigned to implement it.

## What Are The Key Elements Of An Effective Records Retention Program?

Automating email retention should be a key element of an enterprise-wide records management program. Other elements include: the creation of a core team to direct each project, assessment of business and technology requirements, implementation of an email-archiving system, education and training, and monitoring and auditing.

### Create a Core Team

The creation of a records retention policy will be the foundation of a bridge between IT and the legal staff in an organization. In many cases, these individuals will have rarely interacted with each other, but records retention is one shared area of responsibility, and email-archiving is often the first step. Therefore, the first key element of an effective records retention program is a meeting of minds between IT and the legal staff. Additionally, human resources, finance, business functions, and other non-IT individuals are likely to be interested in records retention.

### Assessment

The first action of this joint team will be an assessment of the business and technical needs for record retention. An overall record types inventory must be created for all of the record types found within the organization. Consensus must be developed on the overall e-mail retention policy and gaps between this policy and the reality of email retention must be uncovered. Additionally, the organization's litigation-hold process should be investigated.

The process for dealing with litigation-hold requests and e-discovery should be codified and documented as well. In many cases, IT and legal staff may have previously struggled through e-discovery requests and these lessons can be brought to bear when creating the new methodology. Otherwise, the creativity of the legal and IT staff will be needed to ensure that a reasonable procedure can be put in place to deal with these critical requests on the archiving system.

### Record Retention Policy and Schedule

In some cases, an existing record retention policy may already be in place. The policy should be updated to reflect any new regulations and refreshed to reflect the technical capabilities of the email-archiving system. If a record retention policy and schedule does not exist, now is the time to create one.

A simple record retention schedule can follow the simple logic of the number sequence, 1, 5, 10, 50 and 100. The minimum retention would be 1 year, with most general business correspondence retained for 5 or 10 years. Certain legal, financial, and contract items will require between 5 and 10 years of retention, so they can be placed at 10 years to be on the safe side. Exceptions

## How Long Should Email Be Saved?

requiring longer retention can be placed in a 50 year bucket, which will likely outlast the archive system itself, or could be set with no expiration date. By using a simple retention schedule with just a few time periods, users will more easily understand the implications of their retention choices and overall system management will be simplified.

### Solution Implementation Planning

If an archiving application is not already in place, the team must develop an

overall strategy and implementation plan for such a system. This plan might include vendor and product selections, an RFP, and installation of e-mail archiving software. Although the core team may not be involved at every stage of this implementation, their oversight and energy will be needed to make it a success. Implementation of an email-archiving solution need not wait until the creation of a policy: messages can begin to be stored immediately with no retention decisions made for a number of years.

### Education and Training

Do not under estimate the importance of education and training all users. Regardless of tenure within the organization, all staff must be informed about the new record retention policies being developed and what effort they must put in to ensure compliance. Users must also be trained on how to use the archiving solution and how to manage any retention exceptions.

### Audit

Part of the training should also include awareness of the auditing programs that will report on their effectiveness and the penalties for noncompliance. Long after the policy and technical systems are in place, the core team will continue the process of education and auditing. They must also make sure that any changes to the technical environment, or business and legal requirements, are reflected in the record retention policy.

## Implementing Your New Policies

### Getting Help

With many different archiving software solutions on the market, and many ways to implement them, it can be beneficial to seek out the experience of a consultant or integrator to help put e-mail archiving policies into practice. Consider whether you have the time and

### *Retention Schedule Example*

A retention schedule specifies the amount of time that a given record type will be retained. The example below illustrates a simple policy implementation schedule for different types of e-mail. Although these guidelines may be appropriate for some organizations, each will have to examine their own record retention needs to develop an appropriate schedule.

Default for most emails		5 years
Retention by Department or subject	Product Marketing	5 years
	Legal	10 years
	Human Resources	10 years
	Finance	10 years
	Executive Staff	50 years
	Engineering Development	50 years
	Regulatory Compliance	50 years
Exceptions		Determined by user



## How Long Should Email Be Saved?

experience required to conduct an assessment of archiving needs, develop a retention policy and schedule, plan and implement an archiving product, and train and audit the solution. The software or hardware vendor may be able to recommend an appropriate consulting solution for your needs.

## Using Enterprise Vault

Symantec's popular Enterprise Vault package can be used to automate email retention as discussed above. The system supports integration into multiple email platforms, including Microsoft Exchange and Lotus Domino. Enterprise Vault integrates with the email servers and clients (e.g. Outlook or Lotus Notes). This integration both simplifies user access to messages and allows users to place messages in special retention folders as needed. Administrators have the ability to assign archive folders to users as well as set custom filters using advanced criteria to assign retention exceptions to special content.

The advantages of Enterprise Vault allow administrators begin with a basic blanket policy for most messages. As discussed above, this policy would apply to nearly all messages in the system, but exceptions could be dealt with in one of two ways. The most common implementation includes folder-driven archiving. This is accomplished by having IT push out folders to the user inbox inline with the retention policy. For example, you may have three retention folders created for each user with different categories and retention rules (e.g. Business Records -5yrs; Legal Records - 7yrs; Financial Records -10yrs). Folder-driven archiving enables custom managed folders to which users can move email records with the different requirements. Additionally implementations further enhance classification efforts via custom filters for messages from specific users, such as HR or finance, to extend the protection of these critical communications. Although these techniques will suffice for most cases, some administrators might want to explore the capabilities of custom filters beyond the user or department level, searching on other message metadata and even content. Messages are generally recovered by users as needed, but the archive explorer interface also allows administrators to search for specific content across all users if needed.

If litigation-related discovery is needed, the archive can be explored with the optional Discovery Accelerator module. This module allows designated individuals to execute search queries against the contents of the entire archive in order to produce messages which are determined to be relevant. These searches include message metadata and content, and may relate to specific custodians, usage patterns, and keywords. Discovery accelerator includes a robust litigation hold capability that can be applied to the messages included in the overall search result set. Enabling litigation hold on the contents of the search result set will prevent the archive from deleting this content pursuant to the ongoing execution of the message disposition schedule. The search, review, and preservation workflow of Discovery Accelerator is fully audited and provides a powerful way to respond to legal issues related to email.

## Conclusion

There is no universal solution for the puzzle of e-mail retention or destruction. Laws and regulations are no more clear than internal needs when it comes to deciding how long to keep e-mail messages. Each organization must take a look at the different types of corporate data contained within their e-mail system and develop a policy and schedule to retain and delete messages. Although the answers will vary, each organization should focus on creating a simple and sensible e-mail retention policy.

## How Long Should Email Be Saved?

With e-mail becoming increasingly critical to businesses, interest in e-mail content and handling processes among the legal community was inevitable. No organization can afford to be without a retention policy for e-mail, since this omission could open them to serious penalties from the regulators and litigators.

Although the creation of an overall e-mail retention policy can be complex and time consuming, implementation of an email-archiving system need not wait for it to be completed. In fact, it can be simpler and less risky to simply start collecting all email records immediately rather than trying to create a perfect system and failing. Setting up an archiving solution such as Enterprise Vault prior to the creation of a retention policy may also speed up the policy creation and enforcement process by enabling flexible automated and manual retention methods that would otherwise not be available. Often the best first steps in initiating an email retention policy program are to select an email archiving application compatible with your existing email system and begin archiving all messages without committing to any deletion schedule.

How Long Should Email Be Saved?

## About Contoural, Inc.

Contoural is a leading independent provider of business and technology consulting services focused on litigation readiness, compliance, information and records management, and data-storage strategy. Contoural helps clients address the business requirements emerging around data. For example, electronic discovery rules—under the new Federal Rules of Civil Procedure—now require US companies entering litigation to know what electronically stored information they have, where the ESI is stored, and how quickly they can retrieve that ESI. Similar issues and requirements affect business records in many countries worldwide.

Similarly, legal and regulatory compliance requirements under emerging privacy laws are motivating enterprises to take a closer look at the integrity and security of electronic document files and other digital data. Contoural helps clients understand the business requirements for managing records, and then assists clients to align these business needs with their IT strategies and storage spending. These services bridge the gap between applications and data storage.

Contoural services include:

- Records-retention policy development
- Litigation-discovery process improvement
- Data classification and storage strategy
- Data archiving solution design

With these services, Contoural helps enterprises ensure compliance and reduce risks, while also achieving litigation readiness and reducing costs.

Contoural, Inc.  
1935 Landings Drive  
Mountain View, CA 94043  
650-390-0800  
[www.Contoural.com](http://www.Contoural.com)  
info@contoural.com

How Long Should Email Be Saved?

## About Symantec Enterprise Vault

Symantec Enterprise Vault™ provides a software-based intelligent archiving platform that stores, manages and enables discovery of corporate data from email systems, file server environments, instant messaging platforms, and content management and collaboration systems. Because not all data is created equally, Enterprise Vault utilizes intelligent classification and retention technologies to capture, categorize, index and store target data in order to enforce policies and protect corporate assets while reducing storage costs and simplifying management. Enterprise Vault also provides specialized applications, such as Discovery Accelerator and Compliance Accelerator, that mine archived data to support legal discovery, content compliance, knowledge management, and information security initiatives.

Discovery Accelerator extends the basic search functionality of Enterprise Vault to help lower the cost of data collection and facilitate the search and recovery process of archived items used for electronic discovery. Discovery Accelerator further supports the new Federal Rules of Civil Procedure through configurable enforcement of items during a litigation holds and flexible export capabilities to simplify production. Enterprise Vault is deployed at more than 6000 customers to provide storage management and E-Discovery solutions for more than 8 million mailboxes.

To learn more about how Enterprise Vault and Discovery Accelerator can help IT organizations prepare for the Federal Rules and for the next E-Discovery request please visit [www.symantec.com/enterprisevault](http://www.symantec.com/enterprisevault).



## White Paper

# Six Critical Steps to Managing Electronically Stored Information under FRCP

## Part One: How Legal and IT Can Work Together to Become Litigation Ready

Contoural, Inc.  
1935 Landings Drive  
Mountain View, CA 94043  
[www.contoural.com](http://www.contoural.com)

Sponsored by:



Copyright 2008 Contoural, Inc.

## Six Critical Steps to Managing ESI

### **Abstract**

*Litigation always, has been, and will continue to be, a reality of doing business. What is changing, however, is discovery and its focus on electronically stored information (often abbreviated ESI). Recent amendments to the Federal Rules of Civil Procedure concerning the discovery of ESI coupled with the explosive growth of electronically stored documents are exposing organizations to new risks and costs during litigation and the subsequent discovery.*

*Under these new constraints, organizations need to be aware of these changes, and take specific steps to become litigation ready. Becoming litigation ready is about knowing what ESI you have, where you have it, and how readily you can access it. Retention policies should define defensible data expiration processes, and litigation hold procedures should enable quick and effective preservation of evidence. The best way to manage discovery is to prepare for it before litigation occurs.*

*Becoming litigation ready for ESI cannot be mastered by the Legal group alone. Rather it requires a joint effort between Legal and IT. This pair of white papers list six critical steps both Legal and IT can take to manage ESI.*

*The is the first white paper in a two-part series that covers the following six steps:*

- 1. Create an ESI Survey Data Map*
- 2. Update Your Records Retention and Deletion Policy- and then Execute It*
- 3. Establish Effective Litigation Hold and Discovery Processes*
- 4. Delete Documents that the Business Does Not Need*
- 5. Designate and Prepare a Rule 30(b)(6) Witness*
- 6. Audit Your Process and Periodically Refresh Your Policy*

**Note:** *Legal information is not legal advice. Contoural provides information pertaining to business, compliance, and litigation trends and issues for educational and planning purposes. Contoural and its consultants do not provide legal advice. Readers should consult with competent legal counsel.*

## Six Critical Steps to Managing ESI

### Introduction

Most of an organization's information and documents are either created or received electronically. According to a recent study from UC Berkeley, more than 96% of all information in an enterprise is in digital format, and even 70% of all paper documents are copies of electronic documents. While paper is not going away anytime soon, it typically represents the minority of documents. Litigators have learned that electronically stored information (ESI) can contain significant evidence relevant to a lawsuit, and they target these electronic documents in their discovery efforts. E-mail and other types of ESI are typically the first type of documents targeted in discovery.

Some consider an electronic document such as e-mail not a "real" record. The law takes a different view, as clarified in the December 1, 2006 amendments to the Federal Rules of Civil Procedure (FRCP) that govern court procedures for managing civil suits in the United States district courts. These FRCP changes represented several years of debate at various levels and will have a significant impact on electronic discovery and the management of electronic data within organizations that operate in the United States. These rules regard information stored in electronic form as electronic equivalents of paper documents. This means that in a lawsuit, electronic information is subject to discovery – that is, production to the opposing party – even if the information also is printed in paper form. Companies that cannot locate ESI quickly face severe consequences, including sanctions from the court, or potentially being forced to expand discovery efforts across larger areas within the enterprise.

The best way to manage discovery and avoid these consequences is to prepare for discovery before litigation occurs. The following steps are critical to managing ESI discovery.

### Step 1: Create an ESI Survey Data Map

Perhaps the greatest impact of the FRCP on discovery of ESI is the accelerated timeline for the Rule 26(f) "Meet and Confer" process. Within 100 days of a suit being filed, parties are required to meet and disclose any issues relating to disclosure or discovery of ESI, including form of production, preservation, and privilege/protection issues. This includes the names, types and locations of documents used to support claims. Previously, each side had months, quarters or in some cases years to produce documents. For example, discovery efforts ceased until the resolution of a motion for summary judgement. Considering that often times both inside and outside counsel need to review this information to prepare their strategy, under the new rules, organizations often in reality have only days to weeks to search and retrieve relevant electronic information.

If companies wait until discovery is upon them to start understanding what ESI they have, they run the risk of not locating all relevant information in time. Perhaps more damaging, those who cannot detail what information they have or detail where they have it, or list whether this information may be considered non-accessible, may be forced to search everywhere for relevant information and face an expanded scope of discovery – an expensive and difficult result. In the words of one litigator: "How I come to the Meet and Confer sets the tone for the rest of the trial. If I really know what I have, and where,

### Six Critical Steps to Managing ESI

it sends a strong message to the other side. Likewise, if we aren't as prepared as we should be, that communicates weakness on our part.”

The best preparation should occur before litigation, in creating an ESI Survey Data Map. This is a general enterprise-wide data “map” that lists the types and locations of data across an organization. Often thought of as a “map of the forest” it provides a high-level description of type of documents. This data map is a general, non-case specific tool to enable litigation readiness. Organizations should create such a data map as a general practice, and it should be kept up to date.

**Table 1 - Relevant Electronically Stored Information Systems**

Relevant Electronically Stored Information Systems					
Corporate System Designation	Description	Scope (size)	Character (Data Process Flow)	Organization (data structure or schema)	Data Format(s)
Electronic Mail System	Corporate uses Microsoft Exchange 2003 software for internal and external electronic messaging. This software runs on two Microsoft servers.	There are approximately 2000 Exchange mailboxes with a current message store size of just over 200 GB.	Email messages are routed from the Internet or intranet to the Exchange servers. Microsoft Outlook clients on each workstation access the Exchange server to receive or send messages.	Messages, including SMTP headers and attachments, are stored in the Microsoft Exchange store database. They can be retrieved with the appropriate mailbox access permissions by use of MS Outlook.	Email messages are typically stored in the Microsoft Exchange Message Database. Users also have the ability, through the desktop messaging client MS Outlook, to store messages on their local drive or network share. The format can be MSG for individual
User and Group File Shares	Microsoft Windows Server 2003 is deployed at Corporate to allow centralized management and sharing of desktop application documents.	Documents created by using Microsoft Office are stored on network-attached storage file systems. There are currently about 6,000 GB of such documents.	Corporate users have Microsoft Office applications, such as Word, Excel, PowerPoint, and Access available on their workstations. Documents created by these applications are stored on the network shared file systems.	The desktop application work product files are stored in a standard Windows CIFS structure, with access governed by active directory permission controls.	The network shares store in common Windows file formats, such as .DOC, .XLS, .PPT, etc. and are retrievable using the appropriate MS Office application.
Desktop Personal Computers(PC)	Each user has a pc for network access.	Each PC has a local drive between 50 & 300 GB	Applications run on the local pc's. The MyDocuments folder is re-directed to the network share.	Microsoft Windows XP NTFS file system	PC local drives store in common Windows file formats, such as .DOC, .XLS, .PPT, etc. and are retrievable using the appropriate MS Office application

Source: Contoural, Inc.

Clearly, creation of an ESI Survey Data Map requires close cooperation between Legal and IT. Typically map creation is a joint project between both Legal and IT. Sometimes IT has this information readily available, but often a range of applications and storage systems need to be surveyed and the ESI then needs to be classified and captured within the map.

Companies that produce up-to-date ESI Survey Data Maps will find themselves significantly more litigation ready and able to meet the 100 day “Meet and Confer” deadline. With such a map, they can quickly identify the systems containing responsive information, and dismiss those systems that do not contain relevant information. More important, companies that can create a strong impression in the “Meet and Confer” have a better chance of limiting discovery in inaccessible locations, and also blunt the ability of the opposing party to use discovery as a weapon against them.

### Step 2: Update Your Records Retention and Deletion Policy – and then Execute It

Most companies already have document retention policies in place, but most of these policies are out of date due to a number of factors. First, most document retention policies are focused mainly on paper-based documents, not electronic documents. They were developed around best practices that were in effect at a time when paper was the primary communication and recordkeeping medium. Paper-based documents are treated differently (people don't carry large quantities around with them) and have a different cost structure (storing paper is more expensive). The existing policies do not reflect the “far flung” and multiple-copy nature of email, for example. Also, many of these



## Six Critical Steps to Managing ESI

policies do not reflect the need to preserve information in the event of litigation, or are not clear about which documents should be retained for how long. This lack of clarity can be (and is) exploited by opposing counsel as evidence of a lack of good-faith preservation efforts.

Some of these older policies call for destruction of documents that the currently applicable statutes require preserving, or they specify retention periods that are too short. Equally important, they don't set clear guidelines for deleting older documents that are no longer needed (and that are not subject to preservation under litigation).

In the view of litigators, perhaps worse than an outdated document retention policy – or even no policy – is a policy that is inconsistent or not followed. A typical example of this is a policy that calls for the immediate deletion of all expired documents, while some users still save or print documents. When an opponent during litigation can show that the policy was not followed, this can be used as justification for significantly expanding discovery or to imply that the inconsistent implementation of the policy was due to the company having information to hide. Such an interpretation may be false, but it can play well during litigation.

Companies should update their enterprise document retention policies. Good policies balance different business and legal needs with ease of execution and costs. For electronic documents, policies should favor simpler and fewer retention policies – such that document retention and expiration can be automated to the greatest extent possible. Attributes of good document retention policies include the following:

- *Cover all types of electronic and paper documents* – Good policies cover all types of documents, including e-mail, instant messages, files, and databases as well as paper. Likewise, good policies are comprehensive across the enterprise, including all groups and functional areas, and all types of ESI.
- *Are clear and simple* – Good policies and their corresponding retention schedules tend to be simpler and hence easier to execute, especially for ESI. Good policies are those that can be followed consistently.
- *Can be automated to the greatest extent possible* – The sheer magnitude of electronically stored information requires automation. Where possible, the document retention and discovery should be automated. This starts with having an “automatable” policy.
- *Minimizes manual processes* – Good policies tend to minimize manual processes. Manual processes tend to be more expensive, and it can be very difficult to ensure consistent compliance.
- *Are legally defensible* – Most enterprise document retention policies will be discovered during the course of litigation. The opposing party will be looking to see if the policy was comprehensive and if it was followed. They will be

## Six Critical Steps to Managing ESI

looking to exploit any gaps between what you said you were going to do and what you actually did.

Although policy development is typically led by Legal or Records Management, IT does have an important role. IT needs to educate the Legal group on what are the capabilities of technology and how these would impact proposed policies. Likewise, IT needs to analyze and then educate Legal on the medium and long-term cost implications of various policies. Finally, IT needs to be involved in the development of litigation hold processes to ensure that they can be executed quickly and the results will be defensible. In summary, IT needs to be at the table as the policy is being created.

### Step 3: Effective Litigation Hold and Discovery Processes

The duty to save relevant data starts when notice is received or when a lawsuit could be “reasonably anticipated.” The courts have ruled that duty to preserve documents relevant to litigation begins when companies “knew or should have known” that they were entering litigation. (See box below.) As soon as they enter or have a reasonable belief they will enter litigation, companies should enact a litigation hold, ensuring that all documents relevant to the litigation will be preserved. Legal departments will expect their IT organizations to be able to preserve electronic documents effectively, and be able to locate and retrieve documents quickly.

“Spoliation” is the term used by courts to describe the improper destruction of evidence, including email, messages and other ESI. Companies are guilty of spoliation if they destroy evidence (e.g., company records) relevant to litigation with the purpose or intent of preventing the other party from using the evidence against them. Spoliation can occur both actively (someone shreds documents knowing they are relevant to a case) or passively (through not following the right processes). Unfortunately, spoliation is not always a case of someone consciously deciding to delete evidence. Many cases of spoliation occur through *inactivity* to prevent the destruction of email. This includes failure to stop backup tape rotation, reformatting the laptop from a former employee for a new employee, and deleting old email. Routine electronic document deletion programs must be halted immediately when a business learns there is a reasonable probability of a lawsuit or government investigation. There is an unfortunately long list of *former* CIOs who failed to enact effective hold processes, thus exposing their companies to charges of spoliation. Intent can always be imputed, depending upon the facts.

#### Zubulake vs. UBS Warburg – the ‘Gold Standard’ for ESI Legal Discovery

The duty to save starts when the lawsuit is “reasonably anticipated.” In a 2004 wrongful termination case, for example, an employee filed a claim well after leaving the company. However, the company got in significant trouble with the court for not saving the employee’s emails soon after her departure. The court ruled that although the plaintiff did not file her discrimination charge until August 2001, by April 2001 “almost everyone associated with [the plaintiff] recognized the possibility that she might sue,” and, hence, destruction after that date by the defendant corporation was ruled negligent and resulted in sanctions. This obligation to save also applies to regulatory and grand jury investigations. If the company believes that the company will face litigation on an issue,

## Six Critical Steps to Managing ESI

there is an immediate obligation to begin preserving all messages and documents related to that matter.

Good litigation hold processes require close cooperation between Legal, IT and records custodians. Needless to say, it behooves companies to set up effective litigation hold processes prior to litigation occurring. Good litigation hold processes include the following:

- Determine department / individual responsible for issuing a hold – usually Legal
- How will you communicate a hold action
- Employee acknowledgements of litigation hold
- Date issued
- Scope of the order
- Types of records and any specific content covered
- Locations under hold including potentially employee home workstations
- Employees covered by the notice
- Timeframe covered
- Reason for the order

One common refrain we hear from clients is that even though they may have discoverable messages in many different places, it is unlikely that an opponent's attorneys would know where to look. This is where depositions are playing an important role. Increasingly, we are seeing message administrators and others in IT being called as witnesses in depositions. They are being asked questions such as: "Does the company allow users to save email on the laptops? Do you know any users who do so?" "How many years of backup tapes do you have?" Even if the company has a policy that all email older than sixty days should be deleted, for example, if during the discovery process the opposing party can establish that even a few users saved email on their systems, there is basis to expand the discovery request to all laptops in the organization. We are seeing increasing sophistication in asking the revealing questions in discovery.

How far back does IT need to look in producing email and other electronic documents for discovery? Do you need to find only current email? Often, this is spelled out specifically in the discovery requests and timeframes can go back several years. Increasingly, however, we are seeing discovery requests cover all email, without a specified time frame. This means you need to search for any and all copies of email concerning this issue, regardless of how far back you need to go. In some cases, both parties will agree to specific keywords, meaning that all messages that contain these keywords must be produced. There could be (and are) some requirements for retrieval that go back farther in time than an organization has records to support the request.

Where do you need to look to find email and other documents? For most state courts and regulatory discovery requests, quite simply, everywhere they reasonably may be expected to exist. Under FRCP, this is limited to "reasonably accessible" places. While "reasonably accessible" is the subject of many "Meet and Confer" debates, it is likely to include email servers, PST files on desktops, laptops, copies of email on recent backup tapes, online disaster recovery archives, etc. In the eyes of the court, there is no difference between email contained in an employee's inbox on the server and email

## Six Critical Steps to Managing ESI

located on someone's laptop, even if that someone and his laptop are currently on an extended vacation. There is no protection against having to look in "inaccessible" areas under FRCP. All data locations must be listed. Inaccessible data really means the opponents should have to pay the additional costs of recovering it.

### **Final Thought – The Litigation-Ready Organization**

Nothing can completely prepare an organization for litigation, but the three steps outlined above can reduce the time and energy required to respond when legal issues arise. The process of creating an ESI survey data map, records retention schedule, and litigation hold process will plant seeds of awareness throughout the organization. Employees will begin to consider the implications of their daily actions with regard to electronic documents, and will modify their behavior in a positive way.

This understanding of e-discovery – and the establishment of policies and processes for records retention and litigation hold – will reap enormous benefits, but additional steps can be taken to further prepare for litigation. Most businesses have vast quantities of outdated and superfluous electronic documents that can be removed over time, reducing the volume of data subject to search and discovery. Employees that will be expected to testify to the organization's handling of electronic records can be designated and trained for this role. Processes and policies should also be audited and revisited to ensure that they are kept up to date. These topics are covered further in part two of this whitepaper series.

## Six Critical Steps to Managing ESI

### About Contoural, Inc.

Contoural is a leading independent provider of business and technology consulting services focused on litigation readiness, compliance, information and records management, and data-storage strategy. Contoural helps clients address the business requirements emerging around data. For example, electronic discovery rules—under the new Federal Rules of Civil Procedure—now require U.S. companies entering litigation to know what electronically stored information they have, where it is stored, and how quickly they can retrieve it. Similar issues and requirements affect business records in many countries worldwide.

Similarly, legal and regulatory compliance requirements under emerging privacy laws are motivating enterprises to take a closer look at the integrity and security of electronic document files and other digital data. Contoural helps clients understand the business requirements for managing records, and then assists clients in aligning these business needs with their IT strategies and storage spending. These services bridge the gap between applications and data storage.

Contoural services include:

- Records-retention policy development
- Litigation hold process development
- Litigation-discovery process improvement
- ESI Survey Data Map development
- Data classification and storage strategy
- Data archiving solution design and program management

With these services, Contoural helps enterprises ensure compliance and reduce risk, while also achieving litigation readiness and reducing costs.

Contoural, Inc.  
1935 Landings Drive  
Mountain View, CA 94043  
650-390-0800  
[www.Contoural.com](http://www.Contoural.com)  
info@contoural.com

BY MARK DIAMOND

# EDGE?

## LAWSUITS ARE EXPENSIVE—SO DON'T LET YOUR CONTENT SPIRAL OUT OF CONTROL! SIX STEPS TO HANDLE THAT PESKY “CONTENT ON THE EDGE”

**E**VERY YEAR, BUSINESSES AROUND THE WORLD CREATE more than 7.5 billion documents. Many of these documents live “on the edge”—in laptops, wikis, cell phones, USB drives, instant messages, etc.—floating on the Internet or other hard-to-reach places well out of control. While few of these constitute true business records, many organizations are learning that they can have a huge impact on litigation, regulatory discovery, and privacy breaches.

### WHAT IS THE EDGE AND WHY SHOULD WE CARE?

Companies have long created, managed, and secured documents within official document repositories including email servers, corporate file servers, relational database, and other applications housed and controlled within the four walls of the data center. With the advent of the Internet and then mobile computing, that began to change. Email on cell phones, instant and text messages, laptops, home PCs, and even USB drives have created a type of document diaspora where centrally created information migrates outward. These mobility technologies have advanced much faster than companies' ability to control information moving across them. Employees want, demand, and often get unfettered access to the edge. If denied, they often find a way around restrictions. The edge grows yearly.

Very few documents on the edge are true business records. These few business records that do make it out to the edge typically are copies of documents already in repositories—so why care? While the edge has few records, it does have many, many documents that may contain significant amount of discoverable or sensitive information. What is out there, and your inability to find it quickly, can hurt you. These documents are subject to litigation discovery, regulatory discovery (yes, regulators can request you produce non-records), and some can contain private or other sensitive information.

Documents on the edge are particularly sensitive during litigation discovery for two reasons: First, identification and collection of documents on the edge can be expensive and time-consuming. Discovery often constitutes more than 50 percent of the cost of litigation, often driven by the sheer volume of documents that must be collected and reviewed. It's very difficult to

## Many information managers understand the risk that the edge poses. However, often this problem seems so large that companies freeze—either overwhelmed by the complexity of the task or waiting to perfect a solution before doing anything. That's a mistake.

discover against the edge quickly. Content is the other risk. Employees say the darnedest things on text messages, statements they would never commit to paper or proclaim as company policy. (See “Detroit Mayor Learns the Hard Way,” page 46). These documents, which the authors never deemed would be considered a business document, sometimes come back to haunt both employer and employee.

Many information managers understand the risk that the edge poses. However, often this problem seems so large that companies freeze—either overwhelmed by the complexity of the task or waiting for a perfect solution. That's a mistake. Take steps now to minimize the risk at your company.

### 1. MAP YOUR DEVICES (DON'T BE IN DENIAL)

If you believe your employees have only a few access paths to the edge, you're most likely wrong. Employees have a variety of tricks for accessing the edge, including “unapproved” cell phones with email (especially iPhones), utilizing proxy servers, creating separate archive-only Gmail accounts, etc. There are many devices that you don't control that can connect to your system if you open access for some devices.

Map those devices and all the creative ways employees can access the edge. Be honest—while you may have a corporate policy restricting employees to one type of cell phone, how many carry a second “personal” phone, which still accesses the corporate email server? How common are USB drives?

### 2. CAPTURE IS HALF THE BATTLE

Half of the battle for managing the edge is finding documents already there. Litigators are often fearful of missing something during discovery, and know that many of these reside on the edge. Therefore it is not atypical during document discovery for companies to impound and search cell phones, laptops, and even home PCs. Regardless of whether what you find is helpful or hurtful, often the cost of dis-

covery on the edge is in itself the most burdensome. Many organizations are capturing and copying emails, text messages, instant messages, and other information as it moves out of control, often synchronizing these with existing document repositories. These repositories then represent the copy of record, and any discovery can be performed against them. There is no need to chase down someone's laptop, because a copy already exists in your repository. Unfortunately, often the ability to capture documents requires purchasing someone's software. However, many newer messaging systems, such as those for in-house instant messaging (IM), for example, have logging capability built in.

### 3. IF YOU CAN'T STOP IT MONITOR IT

Once a message or document is created, it is often difficult to stop or control it. Often the best way to stop hurtful information passing over the edge is to make employees wary of ever sending it in the first place.

We have found that if employees know their communications are being monitored, they are much more likely to send more appropriate, less hurtful information. Increasingly many organizations are logging information at the edge, and retaining this for some indefinite period of time (usually a few months). This information is available for review by their manager or HR. Even if these documents are rarely reviewed, the threat that they might be often is enough to curb bad practices. This review need not be limited to just email messages, but also other media including IM, text messages, wikis, etc.

### 4. INSTANT MESSAGING: YOUR BIGGEST RISK?

Measured on a per-message basis, instant messages (IM) represent more risk than almost any other medium. Employees send IMs quickly, often without considering either what they're saying or whether it's appropriate. They view these messages as ephemeral and disposable. IM is

neither. Regulators and courts take a very different view, allowing the opposing side to discover this information wherever it may reside.

Companies are taking two distinct paths for IM. One group says shut it down. They are prohibiting employees from using IM, and blocking access to IM providers through their firewalls. They believe in heading off trouble at the pass. If you believe that your blocking efforts will be successful, this may be a viable option.

Another group is taking a different tact, fearful that blocking IMs will only lead to employees sending work-related messages from their personal accounts using cell phones. In the words of one litigator,

## CAN YOU LOCK EVERYTHING DOWN?

Some organizations take the position that all documents at the edge represent an unacceptable risk, and attempt to lock everything down through a combination of processes and tools. This includes implementing filtering on outgoing email or denying users access to USB drives on their PCs. This is often supported by the use of Data Loss Protection (DLP) software and other tools. While for certain organizations preventing certain types of information from going over the edge (think of customer social security numbers in a financial institution), trying to block all access to everything can be difficult at best. The emerging best practice is to block the easily defined, most critical information (typically privacy-related), while allowing surveillance for the rest. As with any good strategy, there's a balance here.

## DOES RECORDS MANAGEMENT MATTER?

**DETROIT  
MAYOR LEARNS  
THE HARD WAY**

Detroit Mayor Kwame Kilpatrick found out about the edge the hard way. When asked about his relationship with his (female) chief of staff during a whistle-blower lawsuit, Kilpatrick denied any inappropriate relationship. The Detroit Free Press newspaper investigated, subpoenaing more than 14,000 text messages temporarily archived at the Internet service provider through public disclosure laws. Contrary to the mayor's sworn testimony, the messages show otherwise: They arranged trysts in area hotels and on business trips and exchanged messages that were unmistakably sexual. The city was slapped with a \$9 million judgment, and the mayor faces perjury charges. Just because you don't see it doesn't mean it's gone.

"The biggest thing I fear about instant messages is when I don't know what might be out there." The approach of this second group is to bring IM in-house and force employees only to use these internal systems. With the right systems, some purposely auto-delete messages quickly, preventing the employee from accumulating or archiving them. Others save all messages from IM, treating them like email and reviewing them for inappropriate language or content. Either of these approaches will work if executed consistently.

**5. ELIMINATE (MOBILE) PERSONAL ARCHIVES,  
BUT PROVIDE A CENTRALIZED ALTERNATIVE**

Documents outside a centralized archive—such as PST files or files copied to USB drives are by definition out of your control and on the edge. To re-assert control, many organizations are eliminating these "personal" archives. For example, many companies are prohibiting offline email PST files. Some are taking it a step further through the use of Data Loss Protection (DLP) software, preventing the use of USB drives and other devices, but providing SharePoint sites

instead. You want to make it hard enough for employees to save information the wrong way, so that they will use the right archives.

**6. TRAIN, TRAIN, TRAIN**

It's easy to become cynical about employees and their over-the-edge tactics. To be fair, often they don't understand the risks and are just trying to do their jobs. The key to any edge-control strategy is training. Employees have an interest in avoiding risk, both for the organization and themselves. When they understand the real risks of documents on the edge, they tend to be much more careful about what and how they send it. Good training should include a discussion on proper email usage, the discoverability of documents, as well as clearly separating business from personal communication. It almost must discuss acceptable alternatives for sharing and transmitting information. |

**MARK DIAMOND** ([mdiamond@contoural.com](mailto:mdiamond@contoural.com)) is president and CEO for Contoural ([www.contoural.com](http://www.contoural.com)), a consulting firm for storage issues. Mark is a leader in applying the lifecycle services approach to storage.



THE SEDONA CONFERENCE® WORKING GROUP SERIES



# THE SEDONA CONFERENCE® COOPERATION PROCLAMATION

*Dialogue Designed to Move the Law  
Forward in a Reasoned and Just Way*

COPYRIGHT © 2008, THE SEDONA CONFERENCE®

## *The Sedona Conference® Cooperation Proclamation*

*The Sedona Conference® launches a coordinated effort to promote cooperation by all parties to the discovery process to achieve the goal of a “just, speedy, and inexpensive determination of every action.”*

The costs associated with adversarial conduct in pre-trial discovery have become a serious burden to the American judicial system. This burden rises significantly in discovery of electronically stored information (“ESI”). In addition to rising monetary costs, courts have seen escalating motion practice, overreaching, obstruction, and extensive, but unproductive discovery disputes – in some cases precluding adjudication on the merits altogether – when parties treat the discovery process in an adversarial manner. Neither law nor logic compels these outcomes.

With this Proclamation, The Sedona Conference® launches a national drive to promote open and forthright information sharing, dialogue (internal and external), training, and the development of practical tools to facilitate cooperative, collaborative, transparent discovery. This Proclamation challenges the bar to achieve these goals and refocus litigation toward the substantive resolution of legal disputes.

### **Cooperation in Discovery is Consistent with Zealous Advocacy**

Lawyers have twin duties of loyalty: While they are retained to be zealous advocates for their clients, they bear a professional obligation to conduct discovery in a diligent and candid manner. Their combined duty is to strive in the best interests of their clients to achieve the best results at a reasonable cost, with integrity and candor as officers of the court. Cooperation does not conflict with the advancement of their clients’ interests - it enhances it. Only when lawyers confuse *advocacy* with *adversarial conduct* are these twin duties in conflict.

Lawyers preparing cases for trial need to focus on the full cost of their efforts – temporal, monetary, and human. Indeed, all stakeholders in the system – judges, lawyers, clients, and the general public – have an interest in establishing a culture of cooperation in the discovery process. Over-contentious discovery is a cost that has outstripped any advantage in the face of ESI and the data deluge. It is not in anyone’s interest to waste resources on unnecessary disputes, and the legal system is strained by “gamesmanship” or “hiding the ball,” to no practical effect.

The effort to change the culture of discovery from adversarial conduct to cooperation is not utopian.<sup>1</sup> It is, instead, an exercise in economy and logic. Establishing a culture of cooperation will channel valuable advocacy skills toward interpreting the facts and arguing the appropriate application of law.

---

<sup>1</sup> Gartner RAS Core Research Note G00148170, *Cost of eDiscovery Threatens to Skew Justice System*, 1D# G00148170, (April 20, 2007), at <http://www.h5technologies.com/pdf/gartner0607.pdf>. (While noting that “several . . . disagreed with the suggestion [to collaborate in the discovery process] . . . calling it ‘utopian’”, one of the “take-away’s” from the program identified in the Gartner Report was to “[s]trive for a collaborative environment when it comes to eDiscovery, seeking to cooperate with adversaries as effectively as possible to share the value and reduce costs.”).

## Cooperative Discovery is Required by the Rules of Civil Procedure

When the first uniform civil procedure rules allowing discovery were adopted in the late 1930s, “discovery” was understood as an essentially cooperative, rule-based, party-driven process, designed to exchange relevant information. The goal was to avoid gamesmanship and surprise at trial. Over time, discovery has evolved into a complicated, lengthy procedure requiring tremendous expenditures of client funds, along with legal and judicial resources. These costs often overshadow efforts to resolve the matter itself. The 2006 amendments to the Federal Rules specifically focused on discovery of “electronically stored information” and emphasized early communication and cooperation in an effort to streamline information exchange, and avoid costly unproductive disputes.

Discovery rules frequently compel parties to meet and confer regarding data preservation, form of production, and assertions of privilege. Beyond this, parties wishing to litigate discovery disputes must certify their efforts to resolve their difficulties in good faith.

Courts see these rules as a mandate for counsel to act cooperatively.<sup>2</sup> Methods to accomplish this cooperation may include:

1. Utilizing internal ESI discovery “point persons” to assist counsel in preparing requests and responses;
2. Exchanging information on relevant data sources, including those not being searched, or scheduling early disclosures on the topic of Electronically Stored Information;
3. Jointly developing automated search and retrieval methodologies to cull relevant information;
4. Promoting early identification of form or forms of production;
5. Developing case-long discovery budgets based on proportionality principles; and
6. Considering court-appointed experts, volunteer mediators, or formal ADR programs to resolve discovery disputes.

## The Road to Cooperation

It is unrealistic to expect a *sua sponte* outbreak of pre-trial discovery cooperation. Lawyers frequently treat discovery conferences as perfunctory obligations. They may fail to recognize or act on opportunities to make discovery easier, less costly, and more productive. New lawyers may not yet have developed cooperative advocacy skills, and senior lawyers may cling to a long-held “hide the ball” mentality. Lawyers who recognize the value of resources such as ADR and special masters may nevertheless overlook their application to discovery. And, there remain obstreperous counsel with no interest in cooperation, leaving even the best-intentioned to wonder if “playing fair” is worth it.

---

<sup>2</sup> See, e.g., *Board of Regents of University of Nebraska v BASF Corp.* No. 4:04-CV-3356, 2007 WL 3342423, at \*5 (D. Neb. Nov. 5, 2007) (“The overriding theme of recent amendments to the discovery rules has been open and forthright sharing of information by all parties to a case with the aim of expediting case progress, minimizing burden and expense, and removing contentiousness as much as practicable. [citations omitted]. If counsel fail in this responsibility—willfully or not—these principles of an open discovery process are undermined, coextensively inhibiting the courts’ ability to objectively resolve their clients’ disputes and the credibility of its resolution.”).

This “Cooperation Proclamation” calls for a paradigm shift for the discovery process; success will not be instant. The Sedona Conference<sup>\*</sup> views this as a three-part process to be undertaken by The Sedona Conference<sup>\*</sup> Working Group on Electronic Document Retention and Production (WG1):

Part I: Awareness - Promoting awareness of the need and advantages of cooperation, coupled with a call to action. This process has been initiated by The Sedona Conference<sup>\*</sup> Cooperation Proclamation.

Part II: Commitment - Developing a detailed understanding and full articulation of the issues and changes needed to obtain cooperative fact-finding. This will take the form of a “Case for Cooperation” which will reflect viewpoints of all legal system stakeholders. It will incorporate disciplines outside the law, aiming to understand the separate and sometimes conflicting interests and motivations of judges, mediators and arbitrators, plaintiff and defense counsel, individual and corporate clients, technical consultants and litigation support providers, and the public at large.

Part III: Tools - Developing and distributing practical “toolkits” to train and support lawyers, judges, other professionals, and students in techniques of discovery cooperation, collaboration, and transparency. Components will include training programs tailored to each stakeholder; a clearinghouse of practical resources, including form agreements, case management orders, discovery protocols, etc.; court-annexed e-discovery ADR with qualified counselors and mediators, available to assist parties of limited means; guides for judges faced with motions for sanctions; law school programs to train students in the technical, legal, and cooperative aspects of e-discovery; and programs to assist individuals and businesses with basic e-record management, in an effort to avoid discovery problems altogether.

## Conclusion

It is time to build upon modern Rules amendments, state and federal, which address e-discovery. Using this springboard, the legal profession can engage in a comprehensive effort to promote pre-trial discovery cooperation. Our “officer of the court” duties demand no less. This project is not utopian; rather, it is a tailored effort to effectuate the mandate of court rules calling for a “just, speedy, and inexpensive determination of every action” and the fundamental ethical principles governing our profession.

---

## *Judicial Endorsements*

### *as of January 31, 2009*

**ALABAMA**

Hon. John Carroll (Retired)  
Dean, Cumberland School of Law  
Birmingham, AL

**CALIFORNIA**

Hon. Robert Block  
U.S. District Court for the Central District of  
California  
Los Angeles, CA

Hon. Susan Illston  
U.S. District Court for the Northern District of  
California  
San Francisco, CA

Hon. Elizabeth D. Laporte  
U.S. District Court for the Northern District of  
California  
San Francisco, CA

Hon. Louisa S. Porter  
U.S. District Court for the Southern District of  
California  
San Diego, CA

Hon. Carl J. West  
Los Angeles County Superior Court  
Los Angeles, CA

**COLORADO**

Hon. Morris Hoffman  
Colorado 2d Judicial District Court  
Denver, CO

Hon. Craig B. Schaeffer  
U.S. District Court for the District of Colorado  
Denver, CO

**DISTRICT OF COLUMBIA**

Hon. Francis M. Allegra  
U.S. Court of Federal Claims  
Washington, DC

Hon. Herbert B. Dixon, Jr.  
Superior Court of the District of Columbia  
Washington, DC

Hon. John M. Facciola  
U.S. District Court for the District of Columbia  
Washington, DC

Chief Judge Royce C. Lamberth  
U.S. District Court for the District of Columbia  
Washington, DC

Hon. Gregory Mize (Retired)  
Judicial Fellow, National Center for State Courts  
Washington, DC

**ILLINOIS**

Hon. Morton Denlow  
U.S. District Court for the Northern District of Illinois  
Chicago, IL

Hon. Peter Flynn  
Illinois Superior Court  
Chicago, IL

Hon. Nan Nolan  
U.S. District Court for the Northern District of Illinois  
Chicago, IL

Hon. Sidney Schenkier  
U.S. District Court for the Northern District of Illinois  
Chicago, IL

**KANSAS**

Hon. J. Thomas Marten  
U.S. District Court for the District of Kansas  
Wichita, KS

Hon. David Waxse  
U.S. District Court for the District of Kansas  
Kansas City, KS

**LOUISIANA**

Hon. Sally Shushan  
U.S. District Court for the Eastern District of Louisiana  
New Orleans, LA

**MARYLAND**

Hon. Lynne A. Battaglia  
Maryland Court of Appeals  
Annapolis, MD

Hon. Paul W. Grimm  
U.S. District Court for the District of Maryland  
Baltimore, MD

Hon. Michael Mason  
Montgomery County Circuit Court  
Rockville, MD

Hon. Albert Matricciani  
Maryland Court of Special Appeals  
Baltimore, MD

---

*Judicial Endorsements  
as of January 31, 2009 cont.*

**MASSACHUSETTS**

Hon. Timothy Hillman  
U.S. District Court for the District of Massachusetts  
Worcester, MA

**NEVADA**

Hon. Elizabeth Gonzalez  
Nevada Eighth Judicial District Court  
Las Vegas, NV

**NEW JERSEY**

Hon. Katherine Hayden  
U.S. District Court for the District of New Jersey  
Newark, NJ

Hon. John Hughes  
U.S. District Court for the District of New Jersey  
Trenton, NJ

**NEW YORK**

Hon. Frank Maas  
U.S. District Court for the Southern District of New York  
New York, NY

Hon. Andrew Peck  
U.S. District Court for the Southern District of New York  
New York, NY

Hon. Shira Scheindlin  
U.S. District Court for the Southern District of New York  
New York, NY

Hon. Lisa Margaret Smith  
U.S. District Court for the Southern District of New York  
New York, NY

Hon. Richard J. Sullivan  
U.S. District Court for the Southern District of New York  
New York, NY

Hon. Ira B. Warshawsky  
New York Supreme Court, Commercial Division  
Mineola, NY

**NORTH CAROLINA**

Hon. Albert Diaz  
North Carolina Business Court  
Charlotte, NC

Hon. John R. Jolly, Jr.  
North Carolina Business Court  
Raleigh, NC

Hon. Ben F. Tennille  
North Carolina Business Court  
Greensboro, NC

**OHIO**

Hon. John P. Bessey  
Franklin County Court of Common Pleas  
Columbus, OH

Hon. Richard A. Frye  
Franklin County Court of Common Pleas  
Columbus, OH

Hon. Kathleen McDonald O'Malley  
U.S. District Court for the Northern District of Ohio  
Cleveland, OH

**OKLAHOMA**

Hon. Robert Bacharach  
U.S. District Court for the Western District of Oklahoma  
Oklahoma City, OK

Hon. Robin J. Cauthron  
U.S. District Court for the Western District of Oklahoma  
Oklahoma City, OK

**TEXAS**

Hon. Nancy S. Nowak  
U.S. District Court for the Western District of Texas  
San Antonio, TX

**WASHINGTON**

Hon. Barbara Jacobs Rothstein  
U.S. District Court for the Western District of Washington  
Seattle, WA

2009

THE SEDONA CONFERENCE JOURNAL®

# THE PROTECTIVE ORDER TOOLKIT: PROTECTING PRIVILEGE WITH FEDERAL RULE OF EVIDENCE 502<sup>1</sup>

---

*Patrick L. Oot*<sup>2</sup>  
*Verizon Communications*  
*Washington, DC*

## Introduction

In *The Associate*, bestselling novelist John Grisham describes a law firm document review room as a “long dungeon-like room with no windows, a concrete floor, poor lighting, and neat stacks of white cardboard boxes.”<sup>3</sup> A senior associate informs the first year associates entering the room that, “someday in court, it will be crucial for our litigators to tell the judge that we have examined *every* document in this case.”<sup>4</sup> In the days of paper discovery, such reaching declarations to the bench might have been possible, but in today’s computerized world of electronic discovery, such statements might seem outlandish, perhaps even unethical.<sup>5</sup>

When young staffers on Capitol Hill heard that The Judicial Conference was developing policies to reduce the efforts required to protect attorney-client privilege, there was a common sigh of relief. As former law firm associates, many legislative aides remembered the doldrums of document review. Gaining non-partisan support for Federal Rule of Evidence (FRE) 502 from this group was just the start.

This article summarizes the rules reform efforts of hundreds of attorneys, academics, jurists, policy leaders, legislative aides, think tank members, and legislators; many of whom are also members of The Sedona Conference®. Federal Rules policy reform would be impossible without the commitment of these participants. Thanks to their efforts we now have FRE 502, which “reaffirms and reinforces the attorney-client privilege and work product protection by clarifying how they are affected by, and withstand, inadvertent disclosure in discovery.”<sup>6</sup>

I have four main goals in writing this article:

1. To discuss the problem that FRE 502 sought to correct.
2. To correlate that problem to a real-life case in an historical narrative of FRE 502.
3. To provide an overview of the common law surrounding FRE 502.
4. To identify relevant considerations when drafting Protective Orders.

1 Copyright © Patrick L. Oot, 2009 with a worldwide, royalty-free, non-exclusive license (to reproduce, adapt, and distribute) granted by the author to The Sedona Conference®.

2 Patrick Oot is Director of Electronic Discovery and Senior Litigation Counsel at Verizon, and provides legal guidance to the international telecommunications provider on issues involving electronic discovery and disclosure. See <http://www.thosedonaconference.org/people/profiles/OotPatrick>.

3 John Grisham, *The Associate*, 152 (Doubleday) (2009).

4 *Id.*

5 A simple dispute can involve millions of electronic documents. The likelihood that a litigant can actually review *every* document decreases with increasing data volumes. A party signing such an implausible affirmation might face sanctions under Fed. R. Civ. P. 26(g). Similarly, a party making overbroad requests might also confront sanctions. See *Mancia v. Mayflower Textile Servs. Co.*, 253 F.R.D. 354 (D. Md. 2008). (“Rule 26(g) imposes an affirmative duty to engage in pretrial discovery in a responsible manner that is consistent with the spirit and purposes of Rules 26 through 37. In addition, Rule 26(g) is designed to curb discovery abuse by explicitly encouraging the imposition of sanctions. The subdivision provides a deterrent to both excessive discovery and evasion by imposing a certification requirement that obliges each attorney to stop and think about the legitimacy of a discovery request, a response thereto, or an objection”).

6 154 Cong. Rec. H7818 (Sept. 8, 2008) (remarks of Rep. Jackson- Lee).

If you take only one thing from this article, remember this: *The strongest privilege protections and waiver avoidance is granted to those who not only follow the guidance of FRE 502 but also mutually agree upon an adequately drafted Protective Order.*<sup>7</sup> The two devices are not exclusive.

### The Growing Problem of Privilege Review: Volume and Cost

The attorney-client privilege and work product protections act as vital organs to criminal and civil litigation in the United States. By protecting the confidentiality of communications between clients and their attorneys, our legal system encourages free-flowing, candid inquiry in the attorney-client relationship and protects documents prepared by attorneys to assist their clients in litigation.<sup>8</sup>

Prior to the advent of the personal computer, courts struck down blanket privilege protections and required litigants to zealously protect privileged communications by thoroughly reviewing and analyzing document collections prior to producing a final set to an opponent.<sup>9</sup> Document review became the traditional hazing of first-year associates as they protected their client's claim of privilege by mind-numbingly pulling and logging privileged documents from a discreet production set of banker's boxes.<sup>10</sup>

However, as *The Sedona Conference® Best Practices Commentary on the Use of Search and Information Retrieval Methods in E-Discovery* theorizes, "traditional approaches to searching for relevant [or privileged] evidence are no longer practical or financially feasible" in today's electronic universe where we consider it more appropriate to send an e-mail, post a twitter, or clack out a text message rather than make a phone call or (dare I say) meet in person.<sup>11</sup>

We can blame technology for the data deluge. Cheap storage, web applications, and electronic mailboxes that can store a person's lifetime discourse all *Kindle* the fire endangering privilege protection.<sup>12</sup> However, it is not just data. The traditional pre-FRE 502 approach dictates that attorneys screen vast quantities of documents to guarantee that document collections in response to a discovery request do not include a privileged document for fear that a disclosure would waive the privilege for all documents on that subject matter.<sup>13</sup> Fear of waiver forces clients to pay stratospheric litigation data management fees from vendors, steadily increasing hourly rates at law firms compound the problem.<sup>14</sup>

7 The Sedona Conference has undertaken a mission to promote collaboration between parties in discovery. See *The Sedona Conference® Cooperation Proclamation: The Sedona Conference Working Group Series* (July 2008). Available at <http://www.thesedonaconference.org/>. The Federal Rules of Civil Procedure also provide a vehicle for collaboration, see Rule 26(f).

8 The purpose of the attorney-client privilege is to encourage "full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and the administration of justice." *Upjohn Co. v. United States*, 449 U.S. 383, 389, 101 S. Ct. 677, 66 L. Ed. 2d 584 (1981).

9 "The party claiming that the privilege exists bears the burden of proving that it applies to the communication at issue." *Rhodes citing Sampson v. Sch. Dist. of Lancaster*, 2008 WL 4822023, at \*3 (E.D. Pa. 2008) (citing *In re Grand Jury Empanelled Feb. 14, 1978*, 603 F.2d 469, 474 (3d Cir. 1979)). "Because it impedes full and free discovery of the truth, the attorney-client privilege is strictly construed." *Relion, Inc. v. Hydra Fuel Cell Corp.*, 2008 U.S. Dist. LEXIS 98400 (D. Or. Dec. 4, 2008) citing *Weil v. Investment/Indicators, Research & Mgmt., Inc.*, 647 F.2d 18 (1980). (Interestingly, even after FRE 502 was signed into law, many courts recite privilege protection precedent from an era when secretaries used typewriters [i.e. computers were not a primary communications device]. Arguably, the common law will gradually move as parties fine-tune clawback agreements, Protective Orders, and exploit the benefits of FRE 502. The appendix of this commentary includes guidance that litigants can use to help protect privilege while saving costs).

10 See Fed. R. Civ. P. 26(b)(5)(B), (2009).

11 Jason Baron, et al., *The Sedona Conference® Best Practices Commentary on the Use of Search and Information Retrieval Methods in E-Discovery*. The Sedona Conference Journal, 8 Sedona Conf. J. 189, (Fall, 2007). See also, Steve Lorch, *Is Information Overload a \$650 Billion Drag on the Economy?*, December 20, 2007, available at <http://biis.blogs.nytimes.com/2007/12/20/is-information-overload-a-650-billion-drag-on-the-economy/>. (Not only attorneys have trouble managing client data. The phenomenon of "e-mail bankruptcy" is another indicator that users are buried by the data avalanche).

12 The probability for missing a privileged document in a data set increases proportionally as data volumes increase. On March 8, 2009 Google's free "gmail" service permits a user to store up to 7.3 Gb free of charge. Google Terms of Service, <http://www.google.com/accounts/TOS?hl=en>. *The Sedona Conference® Best Practices Commentary on the Use of Search and Information Retrieval Methods in E-Discovery (August 2007)* n.2. ("One gigabyte of electronic information can generate approximately 70,000-80,000 of text pages, or 35 to 40 banker's boxes of documents"). Coincidentally, the "Kindle" is a portable electronic book reader, for a description of the device see Amazon Kindle - Wikipedia, [http://en.wikipedia.org/wiki/Amazon\\_Kindle](http://en.wikipedia.org/wiki/Amazon_Kindle).

13 Baron at 199, n. 13, ("Compare \$1 to store a gigabyte of data with \$32,000 to review it (i.e., assuming one gigabyte equals 80,000 pages, and assuming that an associate billing \$200 per hour can review 50 documents per hour at 10 pages in length, such a review would take 160 hours at \$200/hr, or approximately \$32,000). For a discussion on subject matter waiver, see Ashish Prasad and Vazantha Meyers "The Practical Implications of Proposed Rule 502." *The Sedona Conference Journal*, 8 Sedona Conf. J. 133, (Fall 2007).

14 Although thwarted by the recent economic downturn, history indicates most law firms have increased their rates year-over-year. See Sandhya J. Bathija, *Law Firms' Rates Edge Up Again: Firms are steadily increasing hourly billing rates across the board*. The National Law Journal. December 11, 2006, <http://www.law.com/jsp/article.jsp?id=1165582065881>. (stating perpetual increases) *Distinguished from* Kathy Robertson, "Usual increase in law firm billing rates not happening this year." San Francisco Business Journal Friday, January 23, 2009 (citing a poor economy that affects firms' ability to increase fees) <http://sanfrancisco.bizjournals.com/sacramento/stories/2009/01/26/focus2.html>.



2009

THE SEDONA CONFERENCE JOURNAL®

In short, privilege protection, a fundamental building block of our legal system, is in danger because the cost of protecting it is becoming too great. The increasing expense of privilege review stems from both growing data volumes and escalating attorney fees. As our litigation process becomes more electronic, policy leaders must adapt antiquated rules to address new concerns.

### Rulemaking History: Advisory Committee on the Federal Rules of Evidence

On April 24, 2006, The United States Judiciary Advisory Committee on the Federal Rules of Evidence held a mini-conference inviting a broad-based coalition of judges, academics, and practitioners to discuss the state of privilege protection in litigation and the need for rules reform.<sup>15</sup> After the hearings, the committee approved the proposed new Rule 502 for publication to the general public and scheduled two hearing dates where the committee would consider public testimony.

On January 29, 2007, Anne Kershaw and I joined 22 other speakers in courtroom 24A at 500 Pearl Street in New York to testify before The Advisory Committee about the benefits of Proposed Federal Rule of Evidence 502.<sup>16</sup> We sought to persuade the Advisory Committee to approve the expansion of privilege protection for all parties in litigation and regulatory filings by providing hard data about the true cost of protecting privilege for a single matter.

In the Kershaw-Oot testimony, we described the laborious and tedious process of multi-tier document review that litigants wade-through in an effort to locate relevant documents and to prevent privileged information from disclosure. We stated that both plaintiffs and defendants (like Verizon) use this expensive and time-consuming process in hopes to avoid the (pre-FRE 502) perils that occur when a party inadvertently produces a privileged document. Most importantly, we informed the advisory committee on the true cost of responding to document requests and protecting privilege for a single real-life matter.<sup>17</sup> Verizon spent over \$13.5 million reviewing and logging documents for relevancy and privilege in a single matter.<sup>18</sup>

The “gold-standard” of attorney document analysis does not necessarily amount to a high level of precision when attempting to protect privilege or even review for relevancy.<sup>19</sup> For example, in the *Blair and Maron* study, attorneys over-estimated their ability to create and develop queries to assess the relevancy of 40,000 documents relevant to a transit accident.<sup>20</sup> “Lawyers estimated that their refined search methodology would find 75% of relevant documents, when in fact the research showed only 20% or so had been found.”<sup>21</sup> Additionally, anyone conducting a simple keyword search of the Enron data can find privileged e-mails that attorneys should have withheld from the production.<sup>22</sup>

Not only is manual document review the least efficient method to search for data, it may provide inferior results compared to other available methods.<sup>23</sup> In the preliminary results of its premier study, *The Electronic Discovery Institute* announced that two computer-assisted document review systems had a higher rate of agreement with an original three tier manual attorney review than a second manual attorney review of the same data set.<sup>24</sup> Moreover, the study also concluded that the two

15 The materials for the April 24, 2006 meeting can be found at [http://www.uscourts.gov/rules/Agenda\\_Books.htm](http://www.uscourts.gov/rules/Agenda_Books.htm) The Sedona Conference Advisory Board was represented at the meeting by several members and observers.

16 Anne Kershaw is an attorney, expert, scholar on electronic discovery and processes. See <http://www.akershaw.com>.

17 For a transcript of the testimony, see <http://www.uscourts.gov/rules/2007-01-29-Evidence-Minutes-Transcript.pdf>. For a copy of the PowerPoint presentation presented to the Rules Committee, see [http://ediscoveryinstitute.org/pubs/The\\_Real\\_Cost\\_of\\_Privilege\\_05.pdf](http://ediscoveryinstitute.org/pubs/The_Real_Cost_of_Privilege_05.pdf). The 2005 matter discussed at the hearing required Verizon to collect both electronic and paper documents from 83 employees in ten states. The extracted data set hosted on the e-discovery vendor's servers equaled 1.3 terabytes and yielded 2.4 million documents.

18 See Gartner, RAS Core Research Note G00148170, *Cost of eDiscovery Threatens to Skew Justice System*, 1D# G00148170, (April 20, 2007), at [http://www.akershaw.com/Documents/cost\\_of\\_ediscovery\\_threatens\\_148170.pdf](http://www.akershaw.com/Documents/cost_of_ediscovery_threatens_148170.pdf). (Coincidentally, this 2005 statistic is often often-cited as one of the few data-points available regarding the cost of document review in complex litigation and regulatory filings in the United States). See also Andreas Kluth, *The Big Data Dump*, *The Economist*, August 28, 2008, at [http://www.economist.com/business/displaystory.cfm?story\\_id=12010377](http://www.economist.com/business/displaystory.cfm?story_id=12010377). See also, Daniel Fisher, “The Data Explosion,” *Forbes*, October 1, 2007 at <http://www.forbes.com/forbes/2007/1001/072.html>.

19 For a full, well informed discussion about problems with assessing large data volumes for litigation see Baron, *Supra*.

20 David C. Blair and M.E. Maron, *An Evaluation of Retrieval Effectiveness for a Full-Text Document-Retrieval System*. Communications of the ACM, Volume 28 Number 3, p. 289 (March 1985).

21 For a discussion of the Blair and Maron study, See Baron, *Supra* at 206.

22 See *Enron Broadband Servs., L.P. v. Travelers Cas. & Sur. Co. of Am.* (In re *Enron Corp.*), 349 B.R. 115, 125 (Bankr. S.D.N.Y. 2006). (Although litigants waived attorney-client privilege on those documents in furtherance of fraud, attorneys should have withheld other non-fraudulent attorney-client communications). A searchable database of produced documents in the Enron matter are available at <http://www.enronexplorer.com>.

23 For more information on the analysis of data retrieval systems see The National Institute of Standards and Technology TREC Legal Track (TREC) at <http://trec-legal.umiacs.umd.edu/>.

24 See *Electronic Discovery Institute Study: Effectiveness of Document Review and Analysis Systems for Litigation and Regulatory Response*. (Preliminary Study Results at [http://ediscoveryinstitute.org/pubs/EDI\\_LegalTech\\_2008.pdf](http://ediscoveryinstitute.org/pubs/EDI_LegalTech_2008.pdf).)

computer-assisted methods could have completed the project in one-third of the time at a savings on cost of over 60%.<sup>25</sup> It's not difficult to conclude that computers can replicate query instructions on large data sets more succinctly than fatigued contract attorneys and associates staring at computer monitor for twelve hours per day.

The second half of the Kershaw-Oot testimony discussed alternate less-expensive techniques to protect privilege that would be possible if FRE 502 was enacted. We presented an example of how a litigant could “bucket” or “set-aside” documents that contain law-firm domain names and documents that advanced search engines can flag as potentially privileged.<sup>26</sup> If a producing party had a multi-jurisdictionally enforceable Protective Order under FRE 502 with a claw-back, that party could feel more comfortable rapidly producing or even providing an initial quick-peek to the remaining corpus of data. The parties could also exchange electronically exported logs of the “potentially privileged” withheld bucket. Subsequently, the requesting party could develop better targeted search methods and requests for the set-aside data sets. Allowing litigants to conduct a real initial investigation furthers both a better understanding of the case and the goals of Federal Civil Procedure Rule 1.<sup>27</sup>

### Rulemaking History: Advisory Committee Report

After the public hearings, the Advisory Committee issued a *Report of the Advisory Committee of Evidence Rules* on May 15, 2007 modifying the previously published proposed rule.<sup>28</sup> The report dropped the selective waiver provision, stretched the jurisdiction of the rule (and Protective Orders) to state forums (for disclosures made in federal court) and productions to federal agencies, almost eliminated subject-matter waiver, and instituted guidelines of reasonableness to avoid waiver for inadvertent disclosure.<sup>29</sup>

The report cited precedent that “set out multi-factor tests for determining whether the inadvertent disclosure is a waiver.”<sup>30</sup> Although the report did not codify the inquiry, it included a pentad test drawn from the case law. In determining whether waiver applies for inadvertent disclosures, courts should consider:

1. The reasonableness of the precautions taken;
2. The time taken to rectify the error;
3. The scope of discovery;
4. The extent of discovery; and
5. The over-riding issue of fairness.<sup>31</sup>

The Advisory Committee also provided guidance to courts with additional considerations when interpreting the *reasonableness of the precautions taken*. Interestingly, the additional considerations refresh twenty-year-old waiver tests with elements contemplating the massive data volumes litigants face when managing discovery. The reasonableness considerations include:

1. The number of documents to be reviewed;
2. The time constraints for production;
3. The use of software applications and linguistic tools in screening for privilege; or
4. The implementation of an efficient records management system before litigation.<sup>32</sup>

<sup>25</sup> *Id.*

<sup>26</sup> <http://www.uscourts.gov/rules/2007-01-29-Evidence-Minutes-Transcript.pdf>.

<sup>27</sup> F.R.C.P. 1.

<sup>28</sup> See *Report of the Advisory Committee on Evidence Rules* at [http://www.uscourts.gov/rules/Reports/2007-05-Committee\\_Report-Evidence.pdf](http://www.uscourts.gov/rules/Reports/2007-05-Committee_Report-Evidence.pdf).

<sup>29</sup> *Id.*

<sup>30</sup> *Id.* citing *Lois Sportswear, U.S.A., Inc. Levi Strauss & Co.*, 104 F.R.D. 103, 105 (S.D.N.Y. 1985) and *Hartford Fire Ins. Co. v. Garvey*, 109 F.R.D. 323, 332 (N.D.Cal. 1985).

<sup>31</sup> *Id.*

<sup>32</sup> *Id.*

2009

THE SEDONA CONFERENCE JOURNAL®

Finally, the committee expressly stated that FRE 502 does not require a post production review, but litigants should follow up on any obvious indications of inadvertent production.<sup>33</sup>

### Rulemaking History: "I'm Just a Bill"

Both The Committee on Rules of Practice and Procedure and The Judicial Conference approved the proposed rule for transmittal to Congress.<sup>34</sup> On September 26 2007, Hon. Lee Rosenthal, Chair of The United States Judicial Conference transmitted the resulting proposed FRE 502; developed from over 70 public comments, the testimony of over 20 witnesses, the views of the Subcommittee on Style, and the Advisory Committee's own judgement.<sup>35</sup> The transmittal letter also included a proposed Committee Note that the Judicial Conference sought to include in the legislative history of FRE 502.<sup>36</sup>

Senator Leahy introduced the proposed rule in the Senate on December 11, 2007. On January 31, 2008, the Senate Judiciary Committee approved the bill unanimously without amendment and published its findings to the full Senate with a written report.<sup>37</sup> After incorporating the Advisory Committee Notes, the bill passed in the Senate on February 27, 2008 and The House of Representatives on September 8, 2008. The bill was enacted as Public Law 110-322 on September 18, 2008 to amend the Federal Rules of Evidence to address the waiver of the attorney-client privilege and the work product doctrine.<sup>38</sup>

### FRE 502: At a Glance

The Appendix of this Article contains an official version of Federal Rule of Evidence 502. The table below summarizes its contents:

Federal Rule	Description
502(a)	Limits subject matter waiver of undisclosed documents to instances of intentional disclosure where similar subject communications ought [in fairness] to be considered together.
502(b)	Mandates non-waiver for unintentionally disclosed documents when reasonable steps were taken to prevent disclosure and the producing party took reasonable steps to correct the error.
502(c)	Limits the instances when a litigant can carry a disclosure in a state court proceeding to a federal proceeding.
502(d)	Prescribes the use of Protective Orders and mandates court ordered non-waiver for any other federal or state proceeding.
502(e)	Prescribes the use of Protective Orders by suggesting that confidentiality agreements only bind the parties to the agreement, unless it is incorporated into a court order.
502(f)	Binds state courts to a federal court's determination of non-waiver.
502(g)	Defines attorney-client privilege and attorney work product.

<sup>33</sup> *Id.*

<sup>34</sup> Because the draft rule involved an evidentiary privilege, congressional action was required before the rule could be adopted. See 28 U.S.C. Section 2074(b) ("Any such rule creating, abolishing, or modifying an evidentiary privilege shall have no force or effect unless approved by Act of Congress.").

<sup>35</sup> Letter from Hon. Lee H. Rosenthal to Hon. Patrick Leahy, Hon. Arlen Specter, Hon. John Conyers, Jr., and Hon. Lamar Smith, transmitting Proposed New Federal Rule of Evidence 502 to Judiciary Committee, (September 26, 2007).

<sup>36</sup> *Id.*

<sup>37</sup> S. Rep. No.110-264, (February 25, 2008) ("The rule proposed by the Standing Committee is aimed at adapting to the new realities that accompany today's modes of communication, and reducing the burdens associated with the conduct of diligent electronic discovery.").

<sup>38</sup> See 154 Cong. Rec. S1317 (Feb. 27, 2008) (remarks of Sen. Leahy) ("I ask unanimous consent to have printed in the Record the Judicial Conference's Committee Note to illuminate the purpose of the new Federal Rule of Evidence and how it should be applied."); 154 Cong. Rec. H7818 (Sept. 8, 2008) (remarks of Rep. Jackson- Lee) ("In order to more fully explain how the new rule is to be interpreted and applied, the Advisory Committee also prepared an explanatory note, as is customary, for publication alongside the text of the rule. The text of the explanatory note appears in the Record in the Senate debate."). Administration of George W. Bush, Acts Approved by the President, 1234 (2008).

In short, FRE 502 creates a national standard governing the effect of inadvertent disclosures on the attorney-client privilege.

### FRE 502: The Cases

Coincidentally, judicial interpretations of FRE 502's reasonableness standards have stirred significant response from the legal community.<sup>39</sup> Citing recent decisions, critics of FRE 502 argue that the rule provides little solace to the burden of mounting privilege review costs. However, naysayers forget that the true benefit of FRE 502 derives from the portability of non-waiver rights that a party maintains through a Protective Order. FRE 502 orders grant litigants the ability to better cooperate on the terms of discovery and pave the path for parties to create solid terms to prevent waiver from inadvertent disclosure. A litigant is in the best position if he maps out a response plan to inadvertent disclosures in a fully-vetted Protective Order before documents even change hands.<sup>40</sup> Courts have already ordered litigants to collaborate with one another to address the problematic costs of a privilege review using FRE 502.<sup>41</sup>

Unfortunately, most of the litigants involved in current FRE 502 rulings failed to seek court sanctioned protection early in the discovery process. Thus, the cases to-date rely on disparate interpretations of reasonableness. Below is a sample of the case law invoking FRE 502:

#### Cases Where Courts Protected the Privilege of Inadvertently Disclosed Privileged Communication

##### *Alcon Mfg. v. Apotex, Inc.*

Some courts have set a reasonable standard for protecting privilege by using FRE 502 to empower Protective Orders to find non-waiver. For example, in a patent dispute before the U.S. District Court for the Southern District of Indiana, the court found non-waiver when the plaintiff inadvertently disclosed a privileged document electronically and later complied with the Protective Order by making a good-faith representation that the disclosure was inadvertent and by taking prompt remedial action when they discovered the disclosure.<sup>42</sup> Judge Baker paralleled his ruling of non-waiver to the purpose statement of the FRE 502 Advisory Committee Note.<sup>43</sup> He concluded, "perhaps the situation at hand could have been avoided had plaintiffs' counsel meticulously double or triple-checked all disclosures against the privilege log prior to any disclosures. However, this type of expensive, painstaking review is precisely what new Evidence Rule 502 and the Protective Order in this case were designed to avoid."

##### *Rhoads Industries, Inc. v. Building Materials Corp.*

Other courts tend to rule in favor of protecting privilege under FRE 502 by heavily weighing common law factors after completing a FRE 502 analysis. For instance, in *Rhoads Industries, Inc. v. Building Materials Corp.*, plaintiff (Rhodes) produced over 800 privileged documents and asserted that the production was inadvertent.<sup>44</sup> Although Judge Baylson ruled in favor of waiver for 120 inadvertently produced privileged documents that plaintiff neglected to timely log under FRCP 26(b)(5), the court resisted a ruling of waiver for the inadvertently produced documents that plaintiff included on a privilege log.<sup>45</sup> In his ruling, Judge Baylson applied FRE 502 in conjunction with a

<sup>39</sup> Leonard Deutchman, *First Take on Federal Rule of Evidence 502*, Pennsylvania Law Weekly (December 11, 2008)

<sup>40</sup> Model Protective Order language is available in the Appendix of this article.

<sup>41</sup> *Spieker v. Quest Cherokee, LLC*, 2008 U.S. Dist. LEXIS 88103 at 13 (D. Kan. Oct. 30, 2008) (Magistrate Judge Humphreys recently addressed both collaboration and FRE 502 in *Spieker v. Quest Cherokee*. The court ruled, "Defendant estimates that a "privilege and relevance" review by counsel will cost approximately \$ 250,000. However, Federal Rule of Evidence 502 was recently enacted to reduce the costs of exhaustive privilege reviews of ESI. The parties need to address Rule 502 in any future production and cost discussions.")

<sup>42</sup> *Alcon Mfg. v. Apotex, Inc.*, 2008 U.S. Dist. LEXIS 96630 (S.D. Ind. Nov. 26, 2008).

<sup>43</sup> "Concluding otherwise would undermine one of the main purposes of new Evidence Rule 502, which codifies the primary purpose of the provisions ...of the Protective Order in this case: to address the "widespread complaint that litigation costs necessary to protect against waiver of attorney-client privilege or work product have become prohibitive due to the concern that any disclosure (however innocent or minimal) will operate as a subject matter waiver of all protected communications or information" which is "especially troubling in electronic discovery." *Id.* at 18 citing Fed. R. Evid. 502 Advisory Committee's note.

<sup>44</sup> *Rhoads Industries, Inc. v. Building Materials Corp.*, 254 F.R.D. 216 (E.D. Pa. 2008).

<sup>45</sup> Fed. R. Civ. P 26(b)(5) requires the logging of documents withheld for privilege. Plaintiff first received notice of its 5/13/2008 inadvertent disclosure from Defendant on 6/5/2008. Plaintiff did not submit its final privilege log until 11/12/2008, some 6 months after initial notice. The court called Rhodes' failure to submit a complete privilege log by 6/30/2008 "too long and inexcusable." Judge Baylson cited two cases that might define a reasonable time period to provide an amended privilege log. A court will likely find a two month delay untimely, whereas a court may determine a response of less than a month is prompt. See *Rhodes*, 8-9, comparing *Ger-A-Grip, II, Inc. v. Hornell Brewing Co., Inc.*, 2000 WL 1201385 (E.D. Pa. 2000) to *In re Total Containment, Inc.*, 2007 WL 1775364, at \*8 (Bankr. E.D. Pa. 2007)

multi-part test detailed in *Fidelity & Deposit Co. of Md. v. McCulloch*.<sup>46</sup> Under the five-part *Fidelity* test, Judge Baylson ruled that although four of *Fidelity* factors favored waiver, the final factor, “Whether the overriding interests of justice would or would not be served by relieving the party of its errors,” should be heavily weighted to favor *Rhodes*.<sup>47</sup> The court ruled against waiver concluding, “loss of the attorney-client privilege in a high-stakes, hard-fought litigation is a severe sanction and can lead to serious prejudice.”<sup>48</sup>

Of equal importance to those seeking to protect privilege, twelve days after the court’s ruling of non-waiver of privilege for logged documents under FRE 502, plaintiff sought clarification from the court on how it should qualify *e-mail strings*<sup>49</sup> to determine if the communication appeared on a privilege log prior to June 30.<sup>50</sup> The court ruled that each privileged message within the string must be separately logged in order to claim privilege; a litigant could not merely log the top tier (most recent) message and expect privilege protection for the entire string.<sup>51</sup> However, the plaintiff was not required to indicate that the e-mail was part of a string, as this disclosure could form a “breach of attorney-client privilege because the act of itemization might force parties, by disclosing what was sent to the attorney, also to disclose the nature of the privileged information.”<sup>52</sup> The court supported its ruling with precedent on privilege logging methodology.<sup>53</sup> However, parties seeking the protection of FRE 502 should consider an alternate approach.

The drafters of FRE 502 sought to reduce the costs of litigation by reducing the burden on litigants to protect privilege. Judge Baylson’s ruling on e-mail strings is important to the FRE 502 discussion for several reasons. Privilege review is expensive.<sup>54</sup> Similarly, accounting for privilege by manually logging individual parts of a string is a core component of the *Rhodes* privilege review methodology.<sup>55</sup> Privilege logging is expensive and time consuming because logging individual parts of e-mail strings is programmatically difficult and often technically impossible to provide an accurate representation of who actually received a lower part of the e-mail string.<sup>56</sup>

As a solution to the logging dilemma, parties could collaborate and negotiate for a jointly favorable production and logging methodology in a court approved Protective Order.<sup>57</sup> Under FRE 502, the parties may enforce the Protective Order in federal and state court; thereby avoiding waiver and protecting privilege if the parties followed an agreed upon logging methodology.<sup>58</sup> For example, if the parties agree to a Protective Order using the bucketing and logging methodology outlined in the previously discussed Kershaw-Oot testimony (perhaps agreeing to top-tier logging), the parties could avoid significant expense, share data with greater speed, all while protecting privilege. In the end, *Rhodes* could have shielded against mistakes with a fully vetted Protective Order.

46 *Rhodes supra* citing *Fidelity & Deposit Co. of Md. v. McCulloch*, 168 F.R.D. 516 (E.D. Pa. 1996). (The *Fidelity* test is substantially similar to the test that appeared in the Federal Rules of Evidence Advisory Committee Note.)

47 *Rhodes supra* note 44, at 10.

48 *Rhodes supra* note 44, at 10.

49 An e-mail string is “a series of e-mails linked together by e-mail responses or forwards. The series of e-mail messages created through multiple responses and answers to an originating message. Also referred to as an e-mail thread. Comments, revisions, and attachments are all part of an e-mail string.” *The Sedona Conference® Glossary: E-Discovery & Digital Information Management* 2d ed., available at <http://www.sedonaconference.org>.

50 *Rhodes Industries, Inc. v. Building Materials Corp.*, (Memorandum Re: Clarification of Memorandum Dated November 14, 2008 RE: Privilege Logs of Emails) (November 26, 2008) (As a sanction for failure to timely log documents [as ordered] for six months, the court ordered plaintiff to produce any privileged document not logged prior to June 30, 2008). Fed. R. Civ. P. 26(b)(5) requires a withholding party to log documents withheld for privilege.

51 *Rhodes Industries, Inc. v. Building Materials Corp.*, (Memorandum Re: Clarification of Memorandum Dated November 14, 2008 RE: Privilege Logs of Emails) (November 26, 2008).

52 *Id.* citing generally Paul R. Rice, Attorney Client Privilege in the United States Section 11:6.1 (2d ed. 2008) (providing a general discussion of this issue and citing cases).

53 *Muro v. Target Corp.*, 250 F.R.D. 350 (N.D. Ill. 2007).

54 See n. 24 and Kershaw-Oot testimony *supra*.

55 Fed. R. Civ. P. 26(b)(5). In *Rhodes*, the court found waiver where the producing party failed to log individual parts of an e-mail string. See *Rhodes* (November 26, 2008) *supra*.

56 Logging older messages in a string is difficult. Many e-mail clients (such as RIM’s pervasive Blackberry Enterprise Server) convert parsed data fields (to, from, cc, bcc, etc.) to ASCII text. This conversion of structured data to unstructured text causes the inability to programmatically capture metadata fields for all but the top-tier, most recent message. For instance, when a user forwards an e-mail, the e-mail client converts fielded metadata to ASCII text. The forwarded message will not programmatically capture the metadata from lower-tier messages metadata and will lose the “bcc” field from sent messages that are later forwarded. Another example of this problematic conversion is how fielded names and e-mail addresses change to ASCII aliases in lower-tier older messages. For example, “john.smith@legal.company.com” might convert to merely “John Smith” in the ASCII string. Determining the identity of authors in lower-tier older parts of a string is difficult for litigants analyzing e-mail collections at large companies that have more than one employee with the same name.

57 See Sedona Collaboration Proclamation, *Supra*.

58 In *Rhodes*, Judge Baylson did not preclude alternate court ordered logging options stating, “I have some hesitancy in adopting a broad, black-letter rule.” *Rhodes* (November 26, 2008), *supra* at 6.

***Koch Foods of Alabama, LLC v. General Electric Capital Corp.***

Courts confronting the issue of inadvertent disclosure for the first time or with little state law guidance tend to adopt the balancing test when assessing waiver. For example, in the poultry equipment ownership dispute *Koch Foods of Alabama, LLC v. General Electric Capital Corp.*, District Court Judge Thompson upheld an order of non-waiver that applied the 5-factor test.<sup>59</sup> The court ruled that “if the Alabama Supreme Court were to confront the issue of inadvertent waiver, it would likely adopt the more comprehensive and sensitive totality-of-the-circumstances analysis...But, more importantly, the totality-of-the-circumstances approach allows for a more comprehensive and sensitive assessment of the often complex and sensitive concerns presented in inadvertent waivers.”<sup>60</sup> Judge Thompson’s ruling upheld the magistrate judge’s order of non-waiver where a privileged e-mail was found tucked in middle of 37-page lease agreement contained in a 3,758 page production, the document was included in Koch’s privilege log, and Koch immediately objected and asserted privilege when document presented at deposition of its CFO.<sup>61</sup>

***Laethem Equip. Co. v. Deere & Co.***

Courts may also find non-waiver through a strict FRE 502(b) examination without turning to a five-factor federal common law analysis. In *Laethem Equip. Co. v. Deere & Co.*, the U.S. District Court for the Eastern District of Michigan found non-waiver when plaintiff inadvertently produced two “M&M” disks to defendant that contained privileged attorney-client communication. As neither party argued that the disclosure was anything but inadvertent, the court turned to the additional factors of FRE 502(b) that “sets forth explicit factors for the court to consider” in its analysis.<sup>62</sup>

The court found that plaintiff took reasonable precautions to protect its privilege due to the relatively small inadvertent disclosure in relation to the voluminous discovery produced.<sup>63</sup> Further, “the materials were copied by defense counsel outside of the “inspect and copy” procedure established by the parties, which would have given counsel for plaintiffs the opportunity to conduct a privilege review of the data on the disks prior to turning that data over to defendants.”<sup>64</sup> Finally, the court determined that plaintiff promptly took reasonable steps to rectify the error, as plaintiff’s counsel objected to Defendant’s use of the disclosed materials and demanded their return on multiple occasions in writing starting on the very first day of their disclosure while obtaining an order for their return three weeks after initial knowledge of the inadvertent disclosure.<sup>65</sup> Accordingly, the court found reasonable precautions were taken under FRE 502(b) and ruled that plaintiff did not waive its privilege.

***Heriot v. Byrne***

Courts have also considered vendor error when weighing the factors of an inadvertent disclosure. In the copyright dispute *Heriot v. Byrne*, defendant sought sequestered documents that had been inadvertently produced as a result of a vendor mistake.<sup>66</sup> Defendant argued that plaintiffs’ counsel was “asleep at the switch” by not re-examining the documents received from the vendor.<sup>67</sup> The court ruled against waiver stating that FRE 502, “does not require the producing party to engage in a post-production review to determine whether any protected communication or information has been produced by mistake.”<sup>68</sup> In its analysis, the court further ruled that the disclosing party undertook reasonable precautions to protect privilege when that party enlisted non-lawyers to manually “review the documents prior to production, assigned them codes, and provided them to the Vendor to properly disclose.”<sup>69</sup> In addition, Judge Ashman ruled that plaintiff’s counsel

<sup>59</sup> *Koch Foods of Alabama, LLC v. General Electric Capital Corp.*, 2008 U.S. Dist. LEXIS 3738 (M.D. Ala. Jan. 17, 2008).

<sup>60</sup> *Id.* at 18.

<sup>61</sup> *Id.*

<sup>62</sup> *Laethem Equip. Co. v. Deere & Co.*, 2008 U.S. Dist. LEXIS 107635 at 107728 ( E.D. Mich. Nov. 21, 2008).

<sup>63</sup> *Id.* at 28.

<sup>64</sup> *Id.*

<sup>65</sup> *Id.* at 29.

<sup>66</sup> *Heriot v. Byrne*, 2009 U.S. Dist. LEXIS 22552 (N.D. Ill. Mar. 20, 2009).

<sup>67</sup> *Id.* at 38.

<sup>68</sup> *Id.* (“Plaintiffs had no duty to re-review the documents after providing them to the Vendor. That would be duplicative, wasteful, and against the spirit of FRE 502. Additionally, imposing on disclosing parties a duty to re-review would chill the use of e-vendors, which parties commonly employ to comply with onerous electronic discovery. Against this grain the Court cannot cut.”)

<sup>69</sup> *Id.* at 43.

2009

THE SEDONA CONFERENCE JOURNAL®

took prompt steps to rectify the error when plaintiff's counsel notified defendant's counsel within twenty-four hours of noticing the error and demanded that the defendants destroy those documents; all prior to depositions.<sup>70</sup> Finally, after an *in camera* review, the court reserved its ruling on privilege protection pending a resubmission of the privileged documents and privilege log because defendant's submission was a "befuddling assemblage of documents."<sup>71</sup> The court ordered the defendants to submit an amended privilege log and a revised compilation of documents after they are organized chronologically.<sup>72</sup>

***Preferred Care Partners Holding Corp. v. Humana, Inc.***

Other courts have ruled against waiver for inadvertent disclosure, abandoning a multi-part case law analysis in favor of the direct statutory FRE 502(b) analysis by simply ruling that the two tests are substantially similar; finding non-waiver even when a party failed to meet its discovery obligations pursuant to a scheduling order.<sup>73</sup> In the breach of confidentiality dispute *Preferred Care Partners Holding Corp. v. Humana, Inc.*, Magistrate Judge Simonton conducted an *in camera* review and concluded that four inadvertently produced documents did not constitute waiver.<sup>74</sup> Again, the court found Humana took reasonable precautions to protect its privilege because some of the emails contained a header "**PRIVILEGED ATTORNEY/CLIENT COMMUNICATION**" and Humana's counsel undertook approximately thirty-three hours of privilege review over a three day period.<sup>75</sup> Interestingly, the court conducted a FRE 502(b) analysis, avoiding the common law "overriding interests of justice" test.<sup>76</sup> In doing so, the court evaded an analysis of Humana's sluggish discovery conduct in the case; a factor that might have caused Judge Simonton to order waiver because other courts have weighed the overriding interests of justice heavily.<sup>77</sup> Even so, those courts seem to use this test to rule against waiver of privilege.<sup>78</sup>

***Am. Coal Sales Co. v. N.S. Power Inc.***

Other courts have also ruled in favor of protecting privilege by comparing common law to FRE 502 analysis. For example, in a breach of contract case before the U.S. District Court for the Southern District of Ohio, *Am. Coal Sales Co. v. N.S. Power Inc.*, Defendant included in its Reply in Support of its Motion for Summary Judgment, an e-mail from plaintiff's employee to its in-house attorney.<sup>79</sup> Plaintiff states that the e-mail was a privileged attorney-client communication that was inadvertently disclosed, and plaintiffs sought to strike the e-mail from the record and to enter a Protective Order. Magistrate Judge Able applied the *Nilavar* test and ruled that plaintiff "took reasonable precautions to avoid inadvertent disclosures by having two attorneys review documents prior to production; that inadvertent production of one document out of over 2,000 documents produced does not weigh in favor of waiver; that the extent of the waiver was not great because the document had not worked its way into the fabric of the litigation; that plaintiff took prompt measures to rectify the disclosure; and that the overriding interests of justice and fairness did not conclusively counsel in favor of waiver."<sup>80</sup> The district court ruled that even though Magistrate Judge Abel should have applied FRE 502, his application of the *Nilavar* test was not contrary to law as the *Nilavar* factors were similar to those identified in FRE 502(b) and Advisory Committee Note.<sup>81</sup>

---

<sup>70</sup> *Id.* at 46.

<sup>71</sup> *Id.* at 66.

<sup>72</sup> *Id.* (Many of the documents contain multiple e-mails and forwarded e-mails, an incestuous intermingling of privileged and unprivileged documents. Some of these e-mails are entirely unprotected and can nowise be claimed as covered by the attorney-client privilege")

<sup>73</sup> *Preferred Care Partners Holding Corp. v. Humana, Inc.*, Case No. 08-20424-CIV, "Order Regarding Documents for In Camera Review" (S.D. Fla., April 9, 2009) ("The undersigned...concludes that it is both just and practicable to apply Rule 502 to the case at bar, because PCP does not object to the application of Rule 502 and because there is no substantive difference between the two standards in light of the facts presented in this particular case") (On January 16, 2009, Humana produced 10,000 pages of documents, approximately two months after the expiration of the discovery deadline).

<sup>74</sup> *Id.* (Although the court found non-waiver of four documents, the court ruled that Humana voluntarily waived privilege on one document, as "Humana acknowledged at the April 3, 2009 hearing, it volunteered the details of its so-called "print and purge scheme" in light of the fact that it forms a central component of its defense to PCP's motion for sanctions; and, those details are now a matter of public record").

<sup>75</sup> *Preferred Care Partners*, at 8-9.

<sup>76</sup> *Preferred Care Partners*, at 7 ("Although the final element of the relevant circumstances test – whether the overriding interests of justice would be served by relieving a party of its error – is not incorporated into the Rule 502 test, the undersigned concludes that the application of this aspect of the test to the circumstances in the case at bar would not alter the result").

<sup>77</sup> *See Rhodes, supra.*

<sup>78</sup> *Id.*

<sup>79</sup> *Am. Coal Sales Co. v. N.S. Power Inc.*, 2009 U.S. Dist. LEXIS 13550 (S.D. Ohio February 23, 2009).

<sup>80</sup> *Id.* at 6-47.

<sup>81</sup> *See* Advisory Committee Note, *supra.*

***Reckley v. City of Springfield***

Courts have ruled liberally when determining if reasonable precautions to protect privilege were taken by a disclosing party under FRE 502. For example, in *Reckley v. City of Springfield*, Defendant City of Springfield inadvertently produced five e-mails to plaintiff.<sup>82</sup> Plaintiff's counsel later presented the disclosed documents during deposition and sought to question plaintiff's former supervisor using the disclosed documents. Judge Merz cited FRE 502(b) and ruled that plaintiff took reasonable steps to prevent disclosure because, "at least some of the e-mails in Exhibit 49 have ATTORNEY-CLIENT PRIVILEGED endorsed on them and Defendants' counsel took prompt steps to claim the privilege and seek return of the e-mails after they were disclosed."<sup>83</sup> The Court concluded that the e-mails "retain[ed] their privileged status and plaintiff must deal with them as provided in Fed. R. Civ. P. 26(b)(5)."<sup>84</sup>

***Kumar v. Hilton Hotels Corp.***

Courts have continued to rule liberally against waiver when applying the multi-part test identified in the Explanatory Note of FRE 502(b); even finding non-waiver by interpreting the intent of the producing party's counsel when determining if that party undertook reasonable precautions to protect the privileged material. In the employment discrimination case, *Kumar v. Hilton Hotels Corp.*, Magistrate Judge Pham ruled against waiver of sixty-one inadvertently produced documents where the e-mails were marked "Attorney/Client Privileged Information" and Hilton's counsel attached a note instructing a legal assistant to redact some of the e-mails at issue.<sup>85</sup> Once more, the court weighed counsel's intent to redact and the mere marking of the documents heavily when determining if reasonable precautions were undertaken. The court also ruled that "Hilton promptly took steps to rectify the error and mitigate the damage of the disclosures, as Hilton's counsel immediately contacted Kumar's counsel to notify him of the inadvertent disclosure and to attempt to retrieve the documents. Hilton also took immediate steps to notify the court of this claim by filing the emergency motion. Finally, the number and magnitude of the disclosures in light of the overall document production weigh against waiver."<sup>86</sup>

**Cases Where Courts Ruled in Favor of Waiver for  
Inadvertently Disclosed Privileged Communication**

***Sitterson v. Evergreen Sch. Dist. No. 114***

Yet, courts require a disclosing party to at least take *some* reasonable precautions to protect its privilege. In *Sitterson v. Evergreen Sch. Dist. No. 114*, an appeal from a trial court decision over waiver of documents in an underlying contract dispute, the Court of Appeals of Washington found waiver after invoking FRE 502 to conduct the pervasive "balanced" common law analysis.<sup>87</sup> As neither party argued that the waiver was advertent, the *Sitterson* court moved on to balance five *Allread* factors to decide if the disclosing Defendant waived its privilege on four advisory letters between the District and its attorney.<sup>88</sup> Using the five factored precedent, the court ruled that defendant waived its privilege. First, counsel for the disclosing party "offered no evidence of any precautions he or his office took to prevent the disclosures."<sup>89</sup> Second, the panel was troubled by the "disclosing party's failure to notice or remedy the error until three years after it was made."<sup>90</sup> Third, the court found such a small document production of 439 documents manageable and not the enormous quantity of documents

<sup>82</sup> *Reckley v. City of Springfield*, 2008 U.S. Dist. LEXIS 103663 (S.D. Ohio Dec. 12, 2008).

<sup>83</sup> *Id.*

<sup>84</sup> *Id.*

<sup>85</sup> *Kumar v. Hilton Hotels Corp.*, 2009 U.S. Dist. LEXIS 53387, 9-10 (W.D. Tenn. June 16, 2009). (Magistrate Judge Pham concluded, "the disclosure was inadvertent, as it is clear Hilton intended to redact these portions of the documents prior to production. Hilton took reasonable steps to prevent disclosure, as evidenced by the fact that the Barkley email begins with the words "Attorney/Client Privileged Information" in bold letters, and Hilton's trial counsel attached a note to D000010 and D000013 directing her legal assistant to redact the Barkley email and the numbering prior to producing the documents to Kumar).

<sup>86</sup> *Id.*

<sup>87</sup> *Sitterson v. Evergreen Sch. Dist. No. 114*, 147 Wn. App. 576 (Wash. Ct. App. 2008).

<sup>88</sup> The five factors enumerated in *Allread* are " (1) the reasonableness of precautions taken to prevent disclosure; (2) the amount of time taken to remedy the error; (3) the scope of discovery; (4) the extent of the disclosure; and (5) the overriding issue of fairness." *Id.* at 588 citing *Allread v. Gren.*, 988 F.2d 1425, 1433 (5th Cir. Miss. 1993).

<sup>89</sup> *Id.*

<sup>90</sup> *Id.* at 588-589. See also *In re Grand Jury Investigation of Ocean Transp.*, 604 F.2d 672, 675 (1979) (where documents were turned over one year prior to the assertion of privilege, and they had already been copied, digested, and analyzed by the time of the motion, the court found that "the disclosure cannot be cured simply by a return of the documents. The privilege has been permanently destroyed.").



2009

THE SEDONA CONFERENCE JOURNAL®

that FRE 502 intended to correct by excusing an inadvertent production of privileged documents.<sup>91</sup> Finally, the Court of Appeals ruled that the issue of fairness favored neither party. Defendant's inadvertent disclosures dealt with its counsel's interpretation of plaintiff's contract claim. Because the jury based its award in quantum meruit, the panel concurred that the disclosures did not unjustly prejudice either party.

### *SEC v. Badian*

Not only do courts require a disclosing party to at least take *some* reasonable precautions to protect its privilege, courts require the disclosing party to attempt to rectify the error in a reasonable amount of time. For example in *SEC v. Badian*, Magistrate Judge Eaton applied common law FRE 502 factors to conclude that non-party Rhino waived any claim of privilege for documents inadvertently produced.<sup>92</sup> First, the court stated that it has "been shown no evidence that Rhino or Bryan Cave LLP took any precautions to weed out any possibly privileged documents."<sup>93</sup> Second, the court found the next factor—the extent of disclosures problematic. Rhino originally stated that that as much as 5% (or 3400 documents) of its production contained inadvertently produced privileged material. Even though Rhino later reduced that number to just 260 documents, the court found that "this is still a significant number of documents."<sup>94</sup> Third, the court turned to the amount of time Rhino took to rectify the error. The court determined that Rhino's failure to make any attempt at rectifying the error for five years was an unreasonable time under the *Lois Sportswear* standard.<sup>95</sup> Finally, in analyzing the overarching issue of fairness standard, the court determined there was "no fairness" in precluding the SEC from using the documents produced by Rhino's counsel, but declined to extend waiver beyond those actually produced.<sup>96</sup>

### *Clarke v. J.P. Morgan Chase & Co.*

Some courts have conducted a waiver analysis even after ruling the disclosure was not privileged using an essential element test.<sup>97</sup> In the employment case *Clarke v. J.P. Morgan Chase & Co.*, the court ruled an e-mail was not privileged after conducting a three-factor test as enumerated in *United States v. Construction Prods. Research*.<sup>98</sup> In *Clarke*, the produced e-mail lacked any indication of attorney-client communication on its face.<sup>99</sup> The e-mail did not state that any of the contents were privileged or confidential.<sup>100</sup> Thirdly, the e-mail most likely was beginning an effectuation of a corporate policy change rather than obtaining or providing legal advice.<sup>101</sup> Because of these three factors the court ruled that the e-mail was not privileged.

Coincidentally, even though the court determined the produced e-mail was not privileged, Judge Freeman conducted a further analysis for waiver as if the e-mail was actually afforded the protection of privilege.<sup>102</sup> The court looked to FRE 502(b) and enumerated four common law factors from *Business Integration Services, Inc. v. AT&T Corp.*, that parallel a 502(b) analysis.<sup>103</sup> In applying the *Business Integration Services* test, Judge Freeman ruled that defendant did "not appear to have taken

91 *Sitterson v. Evergreen Sch. Dist. No. 114*, 147 Wn. App. 576 (Wash. Ct. App. 2008)

92 *SEC v. Badian*, 2009 U.S. Dist. LEXIS 9204 (S.D.N.Y. Jan. 26, 2009) (The parties agree that a claim of inadvertence is governed by the four factors set forth in *Lois Sportswear, U.S.A., Inc. v. Levi Strauss & Co.*, 104 F.R.D. 103, 105 (S.D.N.Y. 1985) (Sweet, J.), and its progeny such as *Business Integration Services, Inc. v. AT&T Corp.*, 251 F.R.D. 121, 129 (S.D.N.Y. 2008)).

93 *Id.* at 8.

94 *Id.* at 11.

95 *Id.* at 16 ("Rhino chose to turn over its email files without stating that it was withholding any portions on the basis of privilege [nor did Rhino] provide any internal list in 2003 of any documents that they were withholding from the SEC on the basis of privilege").

96 *Id.* at 17.

97 *Clarke v. J.P. Morgan Chase & Co.*, 2009 U.S. Dist. LEXIS 30719 (S.D.N.Y. Apr. 10, 2009) citing *United States v. Construction Prods. Research*, 73 F.3d 464, 473 (2d Cir. 1996) ("The essential elements that must be shown by a party asserting the attorney-client privilege are: (1) a communication between client and counsel, which (2) was intended to be and was in fact kept confidential, and (3) [was] made for the purpose of obtaining or providing legal advice").

98 *Id.* at 6.

99 *Id.* (the sender was neither an attorney nor his agent; the e-mail did not state that it contained privileged information; the e-mail did not state that any of the information incorporated therein had been obtained from counsel or was based on communications from counsel or even that counsel had been consulted; nor did it state that the policy change reflected in the e-mail was intended to implement a recommendation of counsel).

100 *Id.* at 10 ("the e-mail did not flag that any of its contents, in particular, were privileged and should not be communicated").

101 *Id.* (The court declined a final determination regarding whether the e-mail was drafted for the purpose of conveying or obtaining legal advice because the producing party failed to meet the first two factors) ("Defendant failed to satisfy its burden to show that the recipients of the e-mail would have reasonably understood that they were even receiving legal advice, which was intended to be held in confidence).

102 *Id.* at 13.

103 *Id.* at 14 citing *Business Integration Services, Inc. v. AT&T Corp.*, 251 F.R.D. 121, 129 (S.D.N.Y. 2008). ("These same factors are also generally weighed by the Court in the context of extrajudicial disclosures...More particularly, the Court should consider (1) the reasonableness of the precautions to prevent inadvertent disclosure, (2) the time taken to rectify the error, (3) the extent of the disclosure, [and] (4) an over[arching] issue of fairness and the protection of an appropriate privilege which . . . must be judged against the care or negligence with which the privilege is guarded").

particular care to prevent the dissemination of the e-mail or the supposedly privileged portions of its contents to the reclassified employees.<sup>104</sup> Furthermore, the inadvertently disclosed e-mail was “on top of the stack” of a small production of 532 pages.<sup>105</sup> Judge Freeman stated that the defendant should have become aware and assessed the privileged status of the e-mail at the latest on the date of initial disclosures on September 15, 2008 and at the minimum started an investigation into the privileged nature of the e-mail on the date of production on December 11, 2009.<sup>106</sup> The defendant did neither. The court also ruled the defendant took too much time to rectify the error. “It was not until February 17, 2009, more than two months after the e-mail had been produced by Plaintiffs [and six days after the document was used in plaintiff’s deposition]...that Defendant’s counsel, for the first time, asserted a claim of privilege.”<sup>107</sup> Third, the court determined that the extent of the disclosure was unreasonable given the volume of the document production and location of the e-mail in the collection.<sup>108</sup> Finally, the court weighed the issues of fairness heavily to favor plaintiff, because “plaintiffs should not have been forced to alter their deposition preparation at the last minute, so as to take account of Defendant’s belatedly raised claim.”<sup>109</sup>

### *Relion, Inc. v. Hydra Fuel Cell Corp.*

Other courts have ruled in favor of waiver by unique interpretations of the FRE 502(b) reasonable precautions standard. In *Relion, Inc. v. Hydra Fuel Cell Corp.*, the court ruled that disclosing counsel should have taken “all reasonable means” to protect privilege; a much greater burden than the reasonable precautions standard set out in FRE 502(b).<sup>110</sup> In *Relion*, plaintiff’s counsel sought the return of its client’s privileged documents by seeking enforcement a Protective Order. Plaintiffs inadvertently disclosed a three inch thick file of “question documents” in its production of documents that “occupied over 40 feet of shelf space.”<sup>111</sup> The production was reviewed by counsel prior to production, but the question document folder was inadvertently left in the collection. Magistrate Judge Hubel ruled that because he found no surprise or deception on the part of the receiving party’s counsel, and the disclosing party had several opportunities to inspect the documents in various formats, he “conclude[d] that Relion did not pursue all reasonable means of preserving the confidentiality of the documents produced to Hydra, and therefore that the privilege was waived.”<sup>112</sup>

Coincidentally, the court might have arrived at a different result by applying the five-factor test included in the Legislative History of FRE 502 because four of five factors favored the plaintiff and non-waiver.<sup>113</sup> However, Judge Hubel could have still found waiver using the five factor test by heavily penalizing the plaintiff for “the time taken to rectify the error” and weighing that single factor with more force than the other four. As Judge Baylson’s ruling in *Rhoads Industries, Inc. v. Building Materials Corp.* strongly weighed a single factor [the interest of justice] to conclude non-waiver, here Judge Hubel might be able to weigh a different factor to find waiver.<sup>114</sup> Even so, additional guidance from the courts is necessary to determine how the five factors interplay with one another. Again, litigants should consider negotiated threshold points for each of the five reasonableness factors and include language in the Protective Order to define when privilege is actually waived.

### *AHF Community Development v. City of Dallas*

Some courts may look to the producing party’s failure to act affirmatively on knowledge of inadvertent disclosure. For example, in a unlawful conduct case, *AHF Community Development v. City of Dallas*, plaintiff AFH moved for determination that defendant City of Dallas waived privilege as to emails inadvertently included on disc produced due to conversion to new litigation management software.<sup>115</sup> While the court declined to construe FRE 502 in its opinion, the court enlisted the factors

104 *Clarke* at 14.

105 *Id.* at 15.

106 *Id.*

107 *Id.* at 18.

108 *Id.* at 21 (“it should be noted that the volume of Plaintiff’s discovery was not so large that the e-mail would have been difficult for Defendant to identify. On the contrary, the document’s existence in that production would have been readily apparent”).

109 *Id.*

110 *Relion, Inc. v. Hydra Fuel Cell Corp.*, 2008 U.S. Dist. LEXIS 98400 at 9 (D. Or. Dec. 4, 2008).

111 *Id.* at 7.

112 *Id.* at 9.

113 The Standing Committee Report n. 29 available at [http://www.uscourts.gov/rules/Reports/2007-05-Committee\\_Report-Evidence.pdf](http://www.uscourts.gov/rules/Reports/2007-05-Committee_Report-Evidence.pdf)

114 See Footnote 42, *supra*.

115 *AHF Cmty. Dev., LLC v. City of Dallas*, 2009 U.S. Dist. LEXIS 10603 (N.D. Tex. Feb. 12, 2009).

2009

THE SEDONA CONFERENCE JOURNAL®

of *Allread v. City of Grenada* to rule that the privilege was voluntarily waived.<sup>116</sup> Although the court determined that the disclosure was indeed inadvertent, the court stated that the failure of defendant to act when “emails clearly labeled as attorney-client privileged were marked as exhibits, shown to a witness at deposition, and the subject of substantive questioning – all without objection.”<sup>117</sup> The court therefore ruled that the defendant failed to take reasonable precautions to protect its privilege and also failed to correct the error within a reasonable time.

### Outlook: Effective Use of FRE 502 Protective Orders

In all of the cases stated where a litigant was subject to waiver, had the parties agreed upon a court ordered FRE 502 non-waiver order, the outcome would likely have been different. I have included a brief discussion of the cases where courts have either effectively suggested or entered Rule 502 protective orders to protect against waiver or privilege. These cases also provide evidence of an evolving trend of cooperation in discovery.<sup>118</sup>

#### *Whitaker Chalk Swindle & Sawyer, L.L.P. v. Dart Oil & Gas Corp.*

Federal courts can mandate the use of FRE 502 protective orders to protect privileged when discovery materials contain significant privileged information and there is a fear of disclosure in another court or forum. For example, in an attorney fee dispute, *Whitaker Chalk Swindle & Sawyer, L.L.P. v. Dart Oil & Gas Corp.*, district court Judge Means denied a stay, but evoked FRE 502 to mandate a protective order that would prevent against the disclosure of privileged information from his court in another state court forum.<sup>119</sup> The court ruled, “Dart has not pointed to any reason why a Texas court would not recognize an order entered under Rule 502, nor is this Court aware of a basis for a Texas court to find privileges waived in state proceedings based on a Federal court’s order requiring discovery in a federal case to proceed...Accordingly, it is within this Court’s authority to order discovery to proceed and that by complying with such order Dart has not waived the attorney-client or work-product privilege in the Esperada suit.”<sup>120</sup> Judge Means further assisted the parties by integrating the terms of the protective order into his opinion.<sup>121</sup> In addition to reviewing the Model Protective Order Terms in the appendix of this article, a litigant should consider reviewing Judge Means’s guidance in this opinion when drafting a FRE 502 protective order.

#### *Tremont LLC v. Halliburton Energy Servs.*

Other courts have used FRE 502 to strengthen the effect of confidentiality orders. In *Tremont LLC v. Halliburton Energy Servs.*, Judge Lee Rosenthal entered a Rule 502 order that not only protected privileged information, but restricted the parties from producing a confidential index to “any other person.”<sup>122</sup> Again, a review of Judge Rosenthal’s October 29, 2008 order in this case will provide litigants with additional guidance when negotiating FRE 502 protective orders.<sup>123</sup>

#### *D’Onofrio v. SFX Sports Group, Inc.*

Other courts have used FRE 502 protective orders to aid in the effort for parties to cooperate.<sup>124</sup> For example, in *D’Onofrio v. SFX Sports Group, Inc.* a wrongful termination case, Magistrate Judge John M. Facciola suggested an order protecting defendant’s privileged information even when the defendant agreed to provide the plaintiff’s counsel with attorney notes taken by the defendants under certain conditions.<sup>125</sup> Taking exception to these conditions, the plaintiff’s counsel

116 *Id.* citing *Allread v. City of Grenada*, 988 F.2d 1425 (5th Cir.1993)

117 *Id.* at 16.

118 See *The Sedona Conference® Cooperation Proclamation*: The Sedona Conference Working Group Series (July 2008)

119 *Whitaker Chalk Swindle & Sawyer, LLP v. Dart Oil & Gas Corp.*, 2009 U.S. Dist. LEXIS 15901 (N.D. Tex. Feb. 23, 2009)/

120 *Id.* at 10.

121 *Id.* at 12.

122 *Tremont LLC v. Halliburton Energy Servs.*, 2009 U.S. Dist. LEXIS 27389 (S.D. Tex. Mar. 31, 2009) (“In the present case—the “2008 Case”—this court entered an order under Federal Rule of Evidence 502 to apply to document production. The Rule 502 Order stated that “the Tremont Parties production of the Tremont Index to Halliburton will not constitute any waiver of any privilege of any kind and will not cause the Tremont Parties to be required to produce the Tremont Index to any other person, including but not limited to, Georgia-Pacific Corporation, Milwhite, Inc., or M-I, LLC”).

123 *Tremont LLC v. Halliburton Energy Servs.*, No. 08-1063 at 35 (S.D. Tex. Mar. 31, 2009) (Judge Rosenthal’s FRE 502 protective order is available for download via PACER at <https://ecf.txsd.uscourts.gov/>).

124 See *The Sedona Conference® Cooperation Proclamation*: The Sedona Conference Working Group Series (July 2008).

125 *D’Onofrio v. SFX Sports Group, Inc.*, 256 F.R.D. 277, (D.D.C. 2009).

argued the plaintiff should be granted access to the attorney notes for relevancy determinations. Judge Facciola granted the motion in part, finding the defendants were allowing access to these documents for efficiency's sake not because the plaintiff was entitled to the documents. Of equal importance in this was the use of statistical sampling to identify privilege logging errors.<sup>126</sup> Yet again there emerging problem of search and retrieval touches the privilege issue.

### **Conclusion: From Courts to Effective Protective Orders**

In review, although most courts analyze FRE 502 to rule in favor of non-waiver, the sample cases above interpret the rule differently. Some invoke common law, while others interpret FRE 502 strictly. One court ruled that a disclosing party merely affixing "Attorney-Client Privilege" to a document took reasonable precautions to protect its privilege, while another court ruled that a litigant deploying a thorough attorney review to locate privilege documents waived its privilege because it did not do enough to protect its privilege. Others cases have required a specific privilege logging methodology.

Litigants should avoid the hazardous variability of inadvertent disclosures protected under FRE 502(b). The most effective method to protect a client's privilege is to negotiate with your opponent for a Protective Order with a clawback provision that is now enforceable in both state and federal jurisdictions under FRE 502(d).

The cases in this article highlight a few of the variables that a litigant should consider when drafting a Protective Order. I include sample language in the appendix of this Article which addresses some (but not all) of the salient points a protective order should cover.

### Appendix

#### **Model Protective Order Provisions (as distributed at The 11th Annual Sedona Conference® on Complex Litigation)<sup>127</sup>**

Pursuant to Rule 502 of the Federal Rules of Evidence, the inadvertent disclosure of protected communications or information shall not constitute a waiver of any privilege or other protection (including work product) if the Producing Party took reasonable steps to prevent disclosure and also took reasonable steps to rectify the error in the event of an inadvertent disclosure. The Producing Party will be deemed to have taken reasonable steps to prevent communications or information from inadvertent disclosure if that party utilized either attorney screening, keyword search term screening, advanced analytical software applications and/or linguistic tools in screening for privilege, work product or other protection. In the event of the inadvertent disclosure of protected materials, the Producing Party shall be deemed to have taken reasonable steps to rectify the error of the disclosure if, within thirty (30) days from the date that the inadvertent disclosure was discovered or brought to the attention of the producing party, the Producing Party notifies the Receiving Party of the inadvertent disclosure and instructs the Receiving Party to promptly sequester, return, delete, or destroy all copies of the inadvertently produced communications or information (including any and all work product containing such communications or information). Upon receiving such a request from the Producing Party, the Receiving Party shall promptly sequester, return, delete, or destroy all copies of such inadvertently produced communications or information (including any and all work product containing such communications or information), and shall make no further use of such communications or information (or work product containing such communications or information). Nothing herein shall prevent the Receiving Party from challenging the propriety of the attorney-client, work product or other designation of protection.

<sup>126</sup> *D'Onofrio v. SFX Sports Group, Inc.*, 256 F.R.D. 277, 279 (D.D.C. 2009) ("Defendants also agreed at the hearing to permit plaintiff to test the validity of the privilege log using statistical sampling. Defendants offered to allow plaintiff's expert to select a representative sample, that would be made available to plaintiff's counsel for his review to determine whether the privileges asserted were in fact appropriate. Defendants' offer is conditioned on three criteria with which plaintiff takes issue: (1) the documents be designated "attorneys' eyes only," (2) the sample exclude documents that were created on or after March 17, 2006, and (3) plaintiff's expert tell defendants what method he uses to generate the statistical sample prior to doing so").

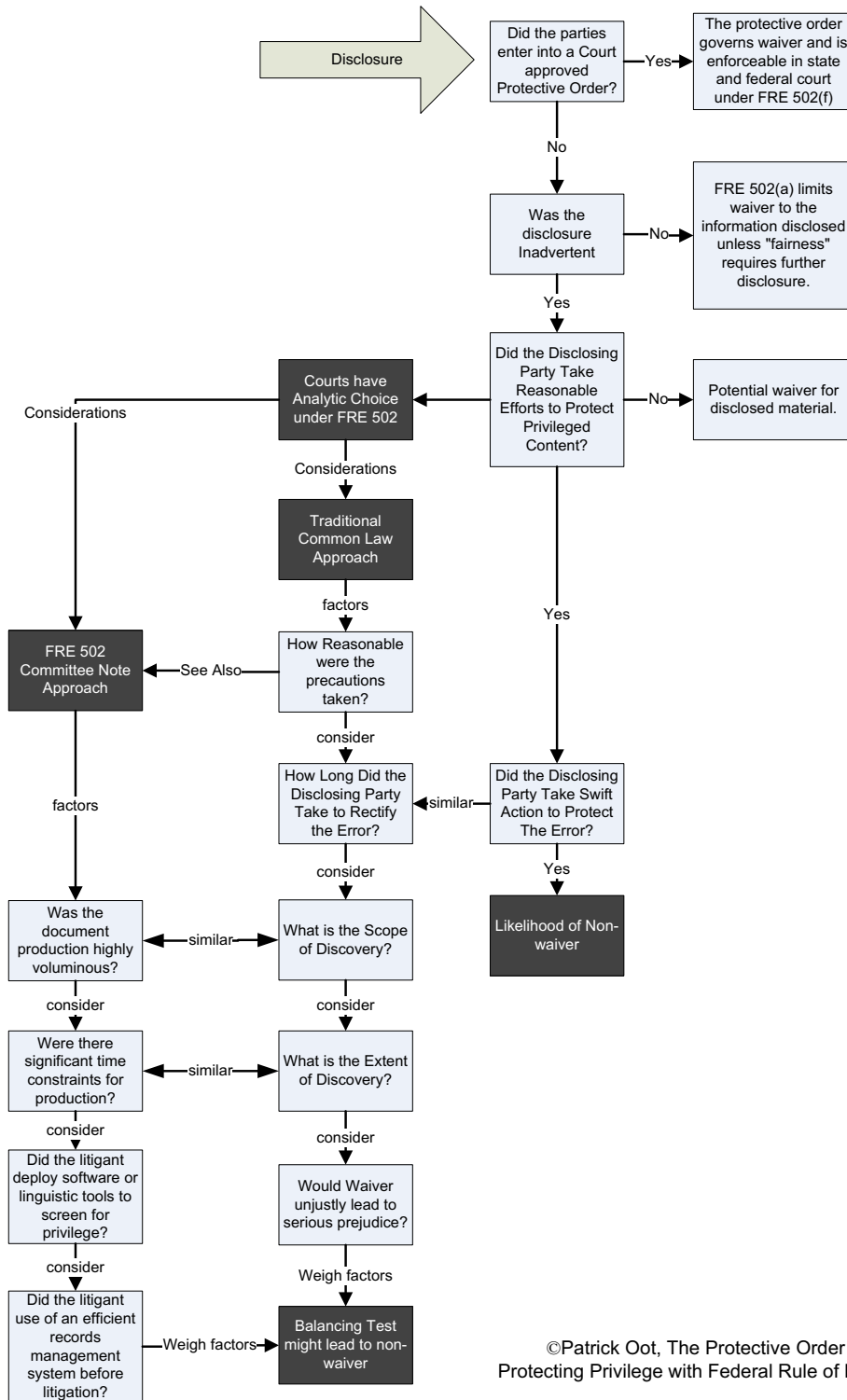
<sup>127</sup> These model protective order provisions were drafted through the collaboration of several active Sedona Conference® members and their colleagues including Tom Allman (Former General Counsel, BASF), Maura Grossman (Wachtell, Lipton, Rosen & Katz), Patrick Oot (Verizon), John Rosenthal, & Charles Molster (Winston & Strawn), Jennifer Tomaino (Verizon), Ken Withers (The Sedona Conference®), and Anne Stukes

2009

THE SEDONA CONFERENCE JOURNAL®

Within 60 days of the production of documents, the parties will provide privilege logs for protected materials withheld for attorney-client privilege or pursuant to the work product doctrine (or other privileges or doctrines). The privilege logs shall contain names or e-mail addresses extracted from the topmost e-mail message or hard copy document (To, From, CC, BCC), the date of the topmost e-mail or document, and the basis for the assertion of a privilege or other protection. The Producing Party shall provide a privilege log for all withheld e-mail or hard-copy documents or other materials [including redacted materials]. The Producing Party shall produce e-mail chains and strings, and shall only redact those portions of the e-mail chain that are protected, leaving all other materials unredacted. The Producing Party shall log all protected content in e-mail chains and strings by logging the topmost e-mail of the e-mail chain or string, as well as sufficient information regarding the redacted material to allow the Receiving Party and the Court to make a cogent evaluation of the appropriateness of the assertion of a privilege or other protection. The Producing Party shall create a single log entry for each e-mail chain or string. A Producing Party's logging of the topmost e-mail shall be deemed to assert protection for all of the protected material in an e-mail string or chain, including multiple redactions or multiple segments. Nothing herein shall prevent the Receiving Party from challenging the propriety of the designation of attorney-client privilege, work product or other designation of protection.

Navigating FRE 502 in Federal Court



©Patrick Oot, The Protective Order Toolkit: Protecting Privilege with Federal Rule of Evidence 502

*Jumpstart Outline*

<http://www.thesedonaconference.org/dltForm?did=Questionnaire.pdf>; and,

*Commentary on Achieving Quality in the E-Discovery Process*

[http://www.thesedonaconference.org/dltForm?did=Achieving\\_Quality.pdf](http://www.thesedonaconference.org/dltForm?did=Achieving_Quality.pdf)

links provided with permission from The Sedona Conference®

## ACC Extras

Supplemental resources available on [www.acc.com](http://www.acc.com)

Small Law: The Rocky Horror Ediscovery Show.

ACC Docket. March 2008

<http://www.acc.com/legalresources/resource.cfm?show=14374>

Corporate Strategies for Reducing Ediscovery Costs.

ACC Docket. February 2008

<http://www.acc.com/legalresources/resource.cfm?show=14403>

Hot Topics in Ediscovery: Are There Any Other Kinds?

Program Material. October 2008

<http://www.acc.com/legalresources/resource.cfm?show=162096>

Please note, these additional resources are provided by the Association of Corporate Counsel and not by the faculty of this session.