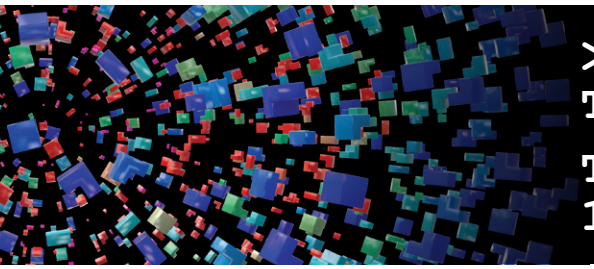

> eDISCOVERY COMPLIANCE AND THE NEW REQUIREMENTS OF IT:

THE IT MANAGER'S GUIDE TO 100% COMPLIANCE

>Authored by Nancy Flynn
Executive Director, The ePolicy Institute
Author, *The e-Policy Handbook, E-Mail Rules, Instant Messaging Rules, Blog Rules, Writing Effective E-Mail, and E-Mail Management*

MessageLabs
SYMANTEC HOSTED SERVICES™

> INTRODUCTION

Symantec Hosted Services – MessageLabs, www.messagelabs.com, and The ePolicy Institute™, www.epolicyinstitute.com, have created this business guide to provide Best-Practices Guidelines for Corporate Compliance with Electronic Discovery Rules.

Through the implementation of a strategic eDiscovery compliance program, incorporating clearly written rules, formal employee education, and a proven-effective Hosted Service Archiving Solution, US and Canadian employers can quickly and cost-effectively preserve, protect, and produce legally compliant email and other Electronically Stored Information (ESI) when compelled to do so by a court or regulatory body.

eDISCOVERY COMPLIANCE AND THE NEW REQUIREMENTS OF IT: THE IT MANAGERS GUIDE TO 100% COMPLIANCE is produced as a general best-practices guidebook with the understanding that neither the author, ePolicy Institute Executive Director Nancy Flynn, nor the publisher, MessageLabs, is engaged in rendering advice on legal, regulatory, or other issues. Before acting on any practice, policy, or procedure addressed in this white paper, you should consult with legal counsel or other professionals competent to review the relevant issue.

> I. EMAIL AND ELECTRONICALLY STORED INFORMATION (ESI) PLAY AN EVER-EXPANDING EVIDENTIARY ROLE: US AND CANADIAN COURTS RAISE THE BAR FOR eDISCOVERY COMPLIANCE

Considering that email and other forms of ESI create the electronic equivalent of DNA evidence, there is no doubt that the evidentiary role of electronic business records will continue to expand. The US federal court system made this clear in 2006, when the much-anticipated amendments to the Federal Rules of Civil Procedure (FRCP) were announced. The amended rules affirm the fact that all ESI—including email messages and attachments—is discoverable and may be subpoenaed and used as evidence—*for or against your organization*—in federal litigation.

The FRCP may apply to Canadian organizations that operate in the US, as well as the Canadian branch offices of American firms.[1]

On the state level, the Golden State became the latest jurisdiction to formalize its own eDiscovery rules when Governor Arnold Schwarzenegger signed California's Electronic Discovery Act (EDA) into law on June 29, 2009. The California law closely (but not exactly) mirrors the 2006 eDiscovery amendments to the FRCP. Passage of the EDA means that electronic discovery will play an increasingly important role in cases that are litigated in California state courts.[2]

California joins about 30 other states that have enacted formal rules to govern the discovery of email and other forms of ESI.[3] It's a safe bet that the remaining 20 states ultimately will follow their lead and enact rules to define the role eDiscovery plays in every state court system.

The discovery of email and other ESI is not limited to litigation in the United States. Electronic discovery is "quickly becoming a factor in all Canadian civil litigation, large and small," according to the The Sedona Conference.[4] Canada, however, has yet to establish national best practice guidelines comparable to the FRCP.[5] Currently, the production of electronic documents in Canadian litigation is governed by each province's rules of civil procedure or rules of court.[6]

eDiscovery Rule:

> Until all remaining states and provinces amend their eDiscovery rules and adopt the FRCP amendments in whole or part, monitor eDiscovery-related developments and rulings in every American state and Canadian province in which your organization has a presence or tries its workplace lawsuits.

In the US, 27% of organizations feel the FRCP amendments have made eDiscovery more challenging, reveals the *Fourth Annual Litigation Trends Survey* from Fulbright & Jaworski L.L.P.[7] To help you navigate the challenges, here's a four-point summary of the FRCP amendments:

1. Within the federal court system and some state courts, email and other forms of ESI are discoverable. That means your retained and archived messages, attachments, and other ESI (business records or not) may be subpoenaed by opposing counsel and used as evidence in workplace lawsuits.

2. Manage electronic data in a manner that allows for its production in a timely, complete, and legally compliant fashion in response to discovery requests during the evidence-gathering phase of litigation.

3. The FRCP amendments do not require your organization to retain *all* email records and *all* other ESI *forever*. Within the ordinary course of business and based on the advice of your legal counsel, you may purge your organization's system of email and other electronic data once it reaches the end of its lifecycle, is no longer needed for regulatory or business reasons, and is not relevant to current, pending, or anticipated legal claims.

4. When it comes to the preservation, purging, and production of email and ESI, the courts appreciate consistency. Establish and adhere to formal retention policies, written deletion schedules, and reliable archiving practices. Doing so will help you deflect potential claims that your organization has illegally destroyed or tampered with electronic evidence.[8]

eDiscovery Rule:

> If you are unclear about the amended FRCP and other laws and regulations governing your organization and industry, have your legal counsel or compliance officer research the matter. Then develop and implement written rules and a formal email/ESI compliance management program—immediately.

> II. 12 LEGAL, REGULATORY, AND BUSINESS REASONS TO RETAIN AND ARCHIVE EMAIL

For unregulated private sector companies, the law does not require the retention of business-related email. Nonetheless, combining a retention policy with a Hosted Service Archiving Solution ensures that your organization's email business records are securely stored and can be readily searched and supplied when needed.

1. Email that is properly managed and securely archived will save you time, money, and stress in the event of litigation. Thanks to archiving technology, you can produce subpoenaed email promptly and responsively.

2. Email creates business records that can protect the organization in the event of a lawsuit. In addition, email records can help shelter you from false claims and unfounded lawsuits.

3. Email evidence that is preserved and produced by your organization may motivate an opponent to settle a weak claim out of court, saving you time and money in the process.

4. Email may provide your organization with the all-important evidence it needs to successfully defend—and win—a workplace lawsuit.

5. Email contains 75% of a company's intellectual property (IP), according to Enterprise Strategy Group research.[9] On average, IP losses cost business over $3,500 per incident. IP retrieval costs may run as high as $500 per incident.[10] Archiving not only helps keep IP safe and secure, but it does so in a cost-effective and legally compliant manner.

6. Email records may enable your organization to take legal or disciplinary action against employees who violate policies, fail to perform, or otherwise act contrary to the best interests of the organization.

7. Email provides a written record that can "*speak*" for witnesses who may be unwilling or unable to testify.

8. Email records can fill in the blanks when human memory falters.

9. Email provides the written records all organizations need in order to operate properly. Formal documentation of transactions, decisions, personnel matters, and day-to-day operations is essential. No entity of any kind can function without reliable records.

10. Email helps keep courts happy. Failure to produce email during discovery may lead to financial and other penalties—if the court believes you intentionally destroyed evidence.

11. Email helps keep government and industry regulators happy. Archiving ensures the automatic preservation of email messages and attachments—and helps you manage the often-complex compliance requirements of multiple regulatory entities.

12. Email archiving guarantees your ability to produce evidence that courts recognize as trustworthy, tamperproof, and authentic. Legally compliant, in other words.[11]

> III. TOP FIVE eDISCOVERY COMPLIANCE TIPS

As part of your organization's email compliance management program, be sure to establish best practices-based rules, policies, and procedures governing the preservation, protection, and production of email and other ESI. Best practices call for the adoption of five eDiscovery compliance tips:

1. Establish a clear definition of "electronic business record" on a company-wide or department-by-department basis. Unfortunately there is no one-size-fits-all definition of "business record." Be sure to involve your legal counsel, compliance officer, IT director, and records manager in the formulation of your definition(s).
2. Communicate the organization's "electronic business record" definition to all employees. Make sure employees can differentiate between business-critical email that must be retained and insignificant non-records that may be deleted. Familiarize users with penalties the organization and individual employees will face should the company fail to meet its eDiscovery and compliance obligations.
3. Know—and adhere to—the electronic record retention and discovery rules imposed by federal, state, provincial, and territorial courts, as well as government and industry regulators.
4. Establish and strictly enforce written rules, policies, and procedures governing the retention and disposition of email messages, attachments, and other ESI.
5. Take advantage of the proven-reliable, cost-effective Hosted Service Archiving Solution from MessageLabs, now part of Symantec, to ensure that incoming, outgoing, and internal messages and attachments are automatically preserved and protected in a legally compliant, tamperproof manner that facilitates the speedy search and responsive retrieval of electronic evidence.[12]

> IV. CONCLUSION: EVERY ORGANIZATION NEEDS eDISCOVERY RULES AND TOOLS

Fully 29% of US organizations were involved in at least one litigation matter in 2007, with 32% battling lawsuits involving $20 million or more, reveals the *Litigation Trends Survey* from Fulbright and Jaworski.[13] In spite of email's growing evidentiary role, however, not all organizations have addressed the need for strategic email management and eDiscovery compliance programs. Only 34% of companies define "electronic business record" for employees, and 33% lack formal email retention policies and deletion schedules, according to American Management Association/ePolicy Institute research.[14]

Your ability to formally define, effectively retain, and successfully archive electronic business records is one of the most important jobs your organization can undertake. Your ability to search for, locate, and produce business-critical email and attachments can have an enormous impact on your organization's assets, reputation, and future should you one day find yourself battling a workplace lawsuit, responding to a regulatory inquiry, or searching for proof of a contested business transaction.[15]

eDiscovery Rule:

> Unmanaged email and other ESI can trigger financial, productivity, and legal nightmares should your organization one day find itself embroiled in a workplace lawsuit. Best practices call for a proactive approach to email management and eDiscovery compliance. Combine written content, usage, and retention policies with a Hosted Service Archiving Solution to ensure your organization's ability to preserve, protect, and produce legally valid email evidence and other ESI.

> V. MESSAGELABS HOSTED SERVICE ARCHIVING SOLUTION

MessageLabs provides a hosted service archiving solution specifically tailored to growing US and Canadian organizations. MessageLabs Hosted Service Archiving Solution is quick to set up, requires no dedicated IT personnel at the company site, offers secure, highly available retrieval of any incoming or outgoing email, and provides a money-back remedy if service availability of 99.9% is not met. As a service, MessageLabs Hosted Service Archiving Solution is a fixed-cost expenditure with no hidden fees and complimentary 24/7/365 technical support.

MESSAGELABS HOSTED SERVICE ARCHIVING SOLUTION FEATURES

- Safe, secure archiving of email and attachments.
- Search and retrieve email and hundreds of types of attachments based on a broad range of criteria or search terms from within Outlook or with a Web-based utility.
- Bounded global search capability can be delegated to legal staff or managers.
- Single-instance storage and stubbing for email and attachments, which helps reduce Exchange data stores by as much as 80%.
- Flexible and customizable supervision and review features that allow compliance staff to monitor, review, and comment on email communications.
- Hosted infrastructure that allows new users and mailboxes to be added easily.
- Avoids archiving viruses and spam when used with MessageLabs Email Anti-Spam and Email Anti-Virus services.

INCREASED PRODUCTIVITY

With efficient email archiving, your legal team can work more productively to conduct search and retrieval of email and hundreds of types of attachments based on a broad range of criteria or search items without the time-consuming intervention of IT specialists or staff.

In addition, attachment stubbing allows IT to meet the needs of end users by essentially removing quotas from their mailboxes. Employees can greatly reduce the time needed to manage email quotas to stay within their mailbox limits. Not only does stubbing make retrieval from MessageLabs servers seamless for end users, but it also frees up valuable storage space on company servers.

REDUCED COSTS

MessageLabs Hosted Service Archiving Solution saves companies IT staff and employee time, storage, hardware, and software investments, while facilitating regulatory compliance measures. All of this cuts costs while improving employee productivity and customer satisfaction

INCREASED PROTECTION

The solution allows administrators to control retention policies by user, group, or message; provides optional supervision and review capabilities; and makes it easy to implement legal holds. With MessageLabs Hosted Service Archiving Solution, once these policies have been put in place, there is no guesswork involved in selecting messages and files for archiving. Employees and management are assured that their correspondence is safely stored and easily retrieved. Because MessageLabs archiving servers are redundant, corporate email is highly available.

ABOUT SYMANTEC HOSTED SERVICES

Symantec Hosted Services is the world's leading provider of hosted services for securing and managing email, Web, and IM traffic (or communications). Over 21,000 organizations and over 9 million end users in 99 countries employ Symantec Hosted Services to protect against viruses, spam, phishing, inappropriate Internet use, spyware and other organization-damaging threats.

ABOUT SYMANTEC

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. More information is available at www.symantec.com

ABOUT THE ePOLICY INSTITUTE™

www.epolicyinstitute.com

The ePolicy Institute is dedicated to helping employers limit email-related risks, including litigation, through effective policies and training programs. The author of 10 books including *The e-Policy Handbook, 2nd Edition,* Executive Director Nancy Flynn is an in-demand speaker, corporate trainer, consultant, and expert witness. Since 2001, ePolicy Institute has collaborated with American Management Association on an annual survey of workplace email/Internet policies, procedures, and best practices. A respected media source, Nancy Flynn has been interviewed by thousands of media outlets including *Fortune, Time, Newsweek, Wall Street Journal, US News & World Report, USA Today, New York Times,* NPR, CBS, CNBC, CNN, NBC, and ABC. For information about ePolicy Institute products and services, contact 614-451-3200 or nancy@epolicyinstitute.com.

REFERENCES

1. Shane Schick, "E-Discovery Rules May Raise E-Mail Issues," *itbusiness.ca* (March 2, 2007), www.itbusiness.ca.
2. Gareth T. Evans, "A Closer Look at Calif. E-Discovery Law," *The Recorder* (July 17, 2009), www.law.com. See also Cheryl Miller, "California Finally Updates E-Discovery Rules, *The Recorder* (July 1, 2009), www.law.com; Glenn Mau and Jeannette Kuo, "California's Electronic Discovery Act 2009," Archer Norris, PLC, www.archernorris.com.
3. David Lender, "California's Electronic Discovery Act," Weil, Gotshal & Manges LLP (July 7, 2009), www.weil.com.
4. Richard G. Braman, "The Sedona Canada Principles: Addressing Electronic Discovery." See "*Preface*," (page i). The Sedona Conference® (January 2008), www.thesedonaconference.org.
5. "The Sedona Canada Principles: Addressing Electronic Discovery." See "*Introduction*," (page 5). The Sedona Conference® (January 2008), www.thesedonaconference.org.
6. "The Sedona Canada Principles: Addressing Electronic Discovery." See "*Introduction*," (page 1). The Sedona Conference® (January 2008), www.thesedonaconference.org.
7. "Fourth Annual Litigation Trends Survey Findings," Fulbright & Jaworski L.L.P. (2007), www.fulbright.com/litigation-trends.
8. Excerpted from Nancy Flynn, *The e-Policy Handbook, Second Edition*, New York, AMACOM, 2009.
9. "E-mail Archiving in the SMB," Enterprise Strategy Group (2008). See also "Email Archiving: A Business-Critical Application," MessageLabs White Paper (2009), www.messagelabs.com.
10. "The Cost of Data Loss," Pepperdine University (2003). See also "Email Archiving: A Business-Critical Application," MessageLabs White Paper (2009), www.messagelabs.com.
11. Tamzin Matthew, "Email Archiving and the Law," Blake Lapthorn Tarlo Lyons, PowerPoint presentation (March 27, 2007), http://www.bllaw.co.uk. See also Nancy Flynn, *The e-Policy Handbook, 2nd Edition*, New York, AMACOM, 2009.
12. Excerpted from Nancy Flynn, *The e-Policy Handbook, Second Edition*, New York, AMACOM, 2009.
13. "Fourth Annual Litigation Trends Survey Findings," Fulbright and Jaworski L.L.P. (2007), www.fulbright.com/litigation-trends.
14. "2009 Electronic Business Communication Policies & Procedures Survey" from American Management Association and The ePolicy Institute. Contact ePolicy Institute Executive Director Nancy Flynn for survey details, nancy@epolicyinstitute.com.
15. Excerpted from Nancy Flynn, *The e-Policy Handbook, Second Edition*, New York, AMACOM, 2009.

>WWW.MESSAGELABS.COM
>INFO@MESSAGELABS.COM
>US AND CANADA: 866 460 0000

>AMERICAS

>UNITED STATES
512 Seventh Avenue
6th Floor
New York, NY 10018
USA
T: 1 866 460 0000

>CANADA
170 University Avenue
Toronto, ON M5H 3B3
Canada
T: 1 866 460 0000

>ASIA PACIFIC

>HONG KONG
Room 3006, Central Plaza
18 Harbour Road
Tower II
Wanchai, Hong Kong
T: 852 2528 6206

>SINGAPORE
6 Temasek Boulevard
#11-01 Suntec Tower 4
Singapore 038986
T: +65 6333 6366

>JAPAN
Akasaka Intercity
1-11-44 Akasaka
Minato-ku, Tokyo 107-0052
Japan
T: + 81 3 5114 4540

>AUSTRALIA
Level 13
207 Kent Street,
Sydney NSW 2000
Australia
T: +61 2 8200 7100

>EUROPE

>UNITED KINGDOM
1270 Lansdowne Court
Gloucester Business Park
Gloucester, GL3 4AB
United Kingdom
T: +44 (0) 1452 627 627

>LONDON
40 Whitfield St
London WIT 2RH
United Kingdom
T: +44 (0) 207 291 1960

>NETHERLANDS
Teleport Towers
Kingsfordweg 151
1043 GR
Amsterdam
Netherlands
T: +31 (0) 20 491 9600

>BELGIUM / LUXEMBOURG
Culliganlaan 1B
B-1831 Diegem
Belgium
T: +32 (0) 2 403 12 61

>GERMANY, AUSTRIA, SWITZERLAND
Feringastraße 9
85774 Unterföhring
Munich
Germany
T: +49 (0) 89 189 43 990

MessageLabs
SYMANTEC HOSTED SERVICES™