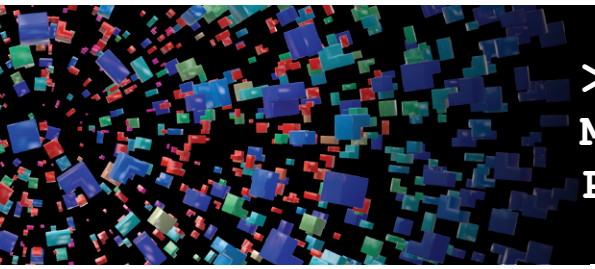

> MASTERING eDISCOVERY: THE IT MANAGER'S GUIDE TO PRESERVATION, PROTECTION & PRODUCTION

>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 for IT Managers 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.

MASTERING eDISCOVERY: THE IT MANAGER'S GUIDE TO PRESERVATION, PROTECTION & PRODUCTION 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. LEGAL RISKS AND RULES: EMAIL AND OTHER ELECTRONICALLY STORED INFORMATION (ESI) CREATE DISCOVERABLE EVIDENCE

Where does your organization stand on the matter of electronic evidence management?

- Do you know the difference between business-critical email that must be retained and archived for legal and regulatory purposes vs. insignificant messages that may be deleted in the ordinary course of business?
- If you are a US company or a Canadian enterprise that deals with the States, are you familiar with the amended Federal Rules of Civil Procedure and any state discovery laws that your organization must comply with?
- If you are a Canadian firm or the Canadian branch of a US company, are you familiar with the eDiscovery rules of the provinces and territories in which you do business?
- In response to a discovery request, could you search, retrieve, and produce legally compliant 7-day-old, 7-month-old, or even 7-year-old email messages and attachments?

If the answer to any of these questions is no, then you had better get to work putting your organization's electronic record management house in order... *right now!*

eDiscovery Rule:

> Your ability to formally define, effectively retain, successfully archive, and promptly produce email and other ESI is one of the most important jobs you can undertake.

> II. DISCOVERY OBLIGATIONS ARE INESCAPABLE: YOU CANNOT AFFORD TO RELAX AND REACT TO THE PROTRACTED AND POTENTIALLY COSTLY DEMANDS OF LITIGATION

During legal discovery, the court orders each party to produce documents relevant to the case. The need to quickly locate and produce legally valid email and other ESI ups the compliance ante for US employers. Fail to meet your discovery obligations, and you could be slapped with a court-imposed financial penalty or other sanction including instructions to the jury to assume that you have intentionally destroyed evidence. Following the lead of the US court system, Canadian courts increasingly are imposing "extraordinary remedies" to discipline parties who fail to meet their eDiscovery obligations, according to The Sedona Conference®. [1]

Real-life eDiscovery Disaster Story:

> In the case of *Z4 Technologies v. Microsoft*, the judge ordered Microsoft to pay damages of $25 million, plus $2 million in attorneys' fees, for litigation misconduct related to the company's failure to produce email evidence and disclose the existence of a database in a timely manner during discovery.[2]

Unmanaged email and other ESI can trigger financial, productivity, and legal nightmares should your organization become embroiled in litigation. The cost and time required to produce subpoenaed email, retain counsel, secure expert witnesses, mount a legal battle, prepare and sit for depositions and trial, cover jury awards and settlements, and launch a PR campaign to salvage your corporate reputation could put you out of business.

Production of subpoenaed email and ESI is mandatory, not an option. Consider these statistics:

- 90% of all business documents generated and acquired are electronic.[3]
- 70% of all that digital information is never converted to hard copy. [4]
- 24% of employers have had employee email subpoenaed by courts or regulatory bodies.[5]

Best practices call for a proactive approach to email management. Follow the lead of the 51% of organizations that have implemented email retention policies and deletion schedules.[6] 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.

eDiscovery Rule:

> Proactive organizations establish strategic email compliance management and eDiscovery programs, combining formal business record retention policies with employee education and proven-reliable archiving technology designed to deliver *cost-effective, comprehensive compliance* with the ever-increasing eDiscovery guidelines of the US federal and state court systems, Canadian provincial courts, and government and industry regulators.

> III. DON'T TAKE CHANCES WITH REGULATORY COMPLIANCE: REGULATORS TAKE SERIOUSLY THE PRESERVATION, PROTECTION, AND PRODUCTION OF ELECTRONIC EVIDENCE

Government and industry regulators have turned an increasingly watchful eye to the content created and business records generated by email, the Web, and other ESI. In fact, 36% of US companies reported increased regulatory inquiries or investigations in 2007. At the same time, 50% of financial services, insurance, engineering, construction, technology, and communications companies saw an upswing in regulatory audits, according to Fulbright & Jaworski research.[7]

Increased use of electronic evidence by regulators and courts has motivated more employers to educate employees about electronic business records, American Management Association/ePolicy Institute research reveals. In 2009, 34% of employers provide employees with a formal definition of "electronic business record," vs. 21% in 2006. As a result, 59% of users claim to know the difference between business-critical messages and insignificant email.[8] Of the 38% of survey respondents who perform a job function that is overseen by government or industry regulators, 61% report adhering to regulatory requirements governing email usage, content, and record retention.[9]

When it comes to records management and eDiscovery, don't take chances with regulatory compliance. Consult with legal counsel to ensure that your organization is in compliance with regulators' email-related rules. Included among the US regulatory bodies and regulations that have established email record retention rules are Sarbanes-Oxley (SOX), Gramm-Leach-Bliley Act (GLBA), SEC, FINRA, Health Insurance Portability and Accountability Act (HIPAA), and the Internal Revenue Service (IRS).

Canadian companies that may be responsible for knowing and complying with SOX, SEC, HIPAA, and other US regulations include those that are listed on the New York Stock Exchange (NYSE), are members of the National Association of Securities Dealers (NASD), or have operations, customers, or patients in the United States.

Canadian firms also must comply with Canadian regulators' email retention and archiving rules. That includes Bill 198, the Canadian version of SOX, and the Personal Information Protection and Electronic Documents Act (PIPEDA), the federal law governing the collection, use, and disclosure of personal information in the course of commercial transactions.[10] In addition, Canadian financial services institutions and professionals must comply with new records management rules imposed by the Canadian Securities Administrators (CSA). Among other requirements, National Instrument 31-103 (NI 31-103) established guidelines for the retention of email and other ESI.[11]

NI 31-103 goes into effect on September 28, 2009.[12]

Those are just a few of many North American regulations and regulators that regularly request access to email. If you are unsure which government or industry regulations govern your employees' use of email, now is the time to find out. Failure to comply could result in seven-figure fines, sinking stock valuations, and shattered reputations among other risks.

> IV. PROTECT THE INTEGRITY OF YOUR EMAIL: WHAT TYPE OF EMAIL MAKES RELIABLE LEGAL EVIDENCE?

To be considered legally valid, the court must deem email to be authentic, trustworthy, and tamperproof. Unfortunately, email can easily be changed—and rendered legally invalid—just by clicking *edit* and *change*. Even all-important business records can be forged when transmitted via email. Unless properly managed and securely archived, email opens your organization to claims ranging from *"I never received your message"* to *"That's not what the attachment said."*[13]

eDiscovery Rule:

> Organizations that are eager to protect email business records are advised to turn to archiving technology to ensure forensic compliance. By instantly encrypting and archiving a copy of every internal and external email sent or received across your organization, a Hosted Service Archiving Solution guarantees that your email is secure and tamperproof. Nothing in your archive can be deleted or altered. Everything in your archive is authentic and legally compliant.

To qualify as a good business record and reliable legal evidence, email must embody five qualities, as detailed in *The e-Policy Handbook, 2nd Edition:*

#1. Authenticity: You can demonstrate who wrote the original message and who altered it.

#2. Integrity: You can prove content and meaning have remained intact since creation.

#3. Accuracy: Throughout its life, legally valid email is accurate about the facts originally documented.

#4. Completeness: Messages and metadata must be intact as part of complete records.

#5. Repudiation: It's easy for a party to claim he did not receive a message or is not responsible for promises made via email. A function of good email evidence, protection against repudiation depends on the reliability of the process used to ensure authenticity, integrity, accuracy, and completeness.[14]

A Hosted Service Archiving Solution assures Authenticity, Integrity, Accuracy, Completeness, and Repudiation—the five essential qualities of compliant records and reliable legal evidence.

> V. 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.[15] In spite of email's growing evidentiary role, 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.[16]

Your ability to formally define, effectively retain, and successfully archive electronic business records is one of the most important jobs you can undertake. Your ability to search for, locate, and produce 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.[17]

eDiscovery Rule:

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

> VI. 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.

For more information visit **www.messagelabs.com/products/archiving**

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. "The Sedona Canada Principles: Addressing Electronic Discovery." See *"Principle 11, Comment 11.b. Canadian Experience to Date with Sanctions,"* (page 36). The Sedona Conference® (January 2008), www.thesedonaconference.org.
2. Eric J. Sinrod, "The New E-Discovery Burden," *CNETNews.com* (October 18, 2007).
3. Kim S. Nash, "E-Mail Retention: The High Cost of Digging Up Data," *Baseline* (August 2, 2006). See also Gareth T. Evans, "A Closer Look at Calif. E-Discovery Law," *The Recorder* (July 17, 2009), www.law.com.
4. Gareth T. Evans, "A Closer Look at Calif. E-Discovery Law," *The Recorder* (July 17, 2009), www.law.com.
5. "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.
6. Ibid.
7. "Fourth Annual Litigation Trends Survey Findings," Fulbright & Jaworski L.L.P. (2007), www.fulbright.com/litigation-trends.
8. "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.
9. Ibid.
10. Wayne Simpson, "E-Mail Compliance: How Much E-Mail Archiving Is Necessary to Comply with Regulations?" *itbusiness.ca* (April 5, 2007), www.itbusiness.ca.
11. Kieron Dowling, "Tough E-Mail Archiving Laws Coming Soon to Canada—and How to Prepare," *itbusiness.ca* (July 8, 2008), www.itbusiness.ca.
12. "NI 31-103 Registration Requirements and Exemptions," www.osc.gov.on.ca/HotTopics/RegReq/ht_regreq_index.jsp.
13. Excerpted from Nancy Flynn, *The e-Policy Handbook, Second Edition,* New York, AMACOM, 2009.
14. Ibid.
15. "Fourth Annual Litigation Trends Survey Findings," Fulbright and Jaworski L.L.P. (2007), www.fulbright.com/litigation-trends.
16. "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.
17. 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™