

The Business Technology Group's Areas of Practice

- ◆ Electronic Records Management
- ◆ Electronic Signatures
- ◆ Information Security and Privacy
- ◆ Intellectual Property
- ◆ IT Disputes and Litigation
- ◆ IT Transactions
- ◆ Outsourcing Transactions

www.lordbissell.com

This brochure is provided solely for educational and informational purposes. It is not intended to constitute legal advice or to create an attorney-client relationship. Readers should obtain legal advice specific to their enterprise and circumstances in connection with each of the topics addressed.

© 2006 Lord, Bissell & Brook LLP

The focus of litigation and investigations on electronic documents, particularly emails, and the increasing court scrutiny of compliance programs, including record retention, are leading organizations to reexamine their management of documents, including their email destruction practices, records management programs, compliance training and monitoring programs, and document creation training. The recognition that electronic messages have become the location both of most business-critical information and of most information-related risk is a recognition of significant new risks, but can lead to significant opportunities for risk and cost management.

Lord, Bissell & Brook LLP assists clients in making the most of their movement to electronic documents, by offering clear, tested project plans for achieving effective e-document policies, practices and technology; enabling avoidance of legal costs and risks through policies, processes and technology; proposing solutions that manage information risks to the desired degrees without interfering in business processes; and reducing vendors' advantages in technology selection, contracting and/or implementation, being—like the vendors—repeat players in those processes.

OVERVIEW

E-Discovery Readiness

Production of electronic documents, particularly messages, has become a costly area fraught with risks for many organizations. For organizations that have not yet confronted the inability of their technology to respond to e-discovery, it is just a “fire in the basement.” Most organizations rely on backup tapes designed for disaster recovery to preserve content from their email systems. Most backup tapes cannot be searched without restoring the whole tape, generally on a server set aside for that purpose. Therefore, when email production requirements were first received in a litigation or investigation, or certain electronic messages became relevant to a reasonably likely litigation or investigation, or when a litigation “hold” was issued by counsel, most organizations had no choice but to start

retaining all of their emails, because the backup tapes or other media did not permit the selective retention that the specific request, hold or area of relevance and good risk management demanded.

Before long, such organizations face a “digital landfill” that lawyers or e-discovery specialists have to pour through at great expense every time new productions are required, preserving in inaccessible form many potentially dangerous documents not relevant to any likely investigation or litigation. And even if the organizations manage to put an end to this landfill through outsourcing it to an e-discovery vendor or escaping the litigation or investigation, all they have accomplished is to provide their adversaries with better access to their information than they provide to those they trust to run their businesses.

Most organizations also impose mailbox size quotas on their users. Email users usually respond by copying messages to their local drives, where they are then kept indefinitely, accessible to others in the organization only with difficulty. The practice of most end-users to retain large amounts of email for personal recordkeeping, to enhance productivity through models for subsequent messages or to justify their actions is usually underestimated.

Seeing organizations making substantial expenditures to produce email and other electronic documents in litigation and investigations without effectively mitigating risk, and getting little if any business value out of those expenditures, Lord, Bissell & Brook has organized a practice to help our clients avoid those costs, better manage the substantial risks of e-discovery and address other key risks related to electronic documents.

We believe that the greatest value is often derived not by tackling e-discovery readiness in a vacuum, but by considering record retention requirements and broader compliance requirements, risk management priorities and business needs to choose the right policies, “search”

criteria and processes and technology for your business. Technology is moving rapidly toward permitting e-document production through defensible automatic processes with limited manual review. These processes and technologies should complement the processes and technology necessary for the organization to keep and find the documents it will continue to need either for business purposes, or as historical records, and to permit monitoring compliance with the multitude of organizational information and communication policies, including protecting the organization against “leakage” of confidential, proprietary or personal information. Our approach to e-discovery readiness is thus integrally linked to (1) information security, (2) records and information management and (3) compliance more generally.

The most dangerous emails from the e-discovery standpoint tend not to be records, however, but rather the informal emails containing thoughtlessly colorful words that can be taken out of context as, e.g., defamation or admission of a violation of law or policy. Policies and training on responsible creation of emails are nothing new, of course; due to emails’ false sense of privacy and ease of use, however, those policies and trainings are often forgotten. Therefore, our e-discovery readiness programs often include training programs that go much farther than anything employees have ever heard to impress them with the legal risks of electronic communication and best practices in document creation. Helping to make those training programs memorable are more stringent sanctions, consistently applied, more regular monitoring of employee emails—sometimes using the same search capabilities noted above to avoid false positives and protect privacy—and more specific notice of that monitoring.

Records Management: New Risks and Approaches

Records management used to be a relatively low-risk, technical area. Retention requirements were generally set based solely on regulatory requirements. Dealing with paper documents that fit into neat categories, it was easy to imagine that files could be kept for the required period and then destroyed. In any event, the achievements and effectiveness of compliance programs were not assessed at all as carefully as they are now.

Our clients understand that their records management programs and email destruction policies need to change because:

- ◆ Most of their business-critical information is now in their email systems;
- ◆ There are vastly more emails than there are paper documents;

- ◆ Emails and other e-messages do not fit into neat retention categories;
- ◆ Electronic records management has become a high-risk area; and
- ◆ Many old record retention policies do not contemplate or implement any process for litigation “holds” for records related to likely litigations or investigations.

Records management programs can thus no longer be merely driven by regulatory requirements, but must be effective at managing many types of risks. We summarize the ten goals of an adequate records management program as that the program must:

1. Be clear and well-suited to employee communication and training;
2. Be administrable given the tremendous volume of electronic messages flowing through your organization;
3. Include monitoring and/or auditing;
4. Filter out unnecessary content to an acceptable yet defensible degree;
5. Rely on the right combination of “end-user” action, automatic processes and post-send records management staff activity;
6. Not compromise speed or productivity;
7. Involve search capabilities that are defensible for e-discovery purposes (i.e., obviate the need for lawyers or e-discovery specialists to review all of your emails) and also serve your business needs;
8. Involve secure storage and transmission;
9. Be capable of adjustment by the client based on changing needs, and
10. Be cost-justifiable in relation to all alternative approaches.

Records management programs must also be based, of course, on extensive knowledge regarding legal retention periods, as well as legal and business needs for records integrity and security. Integral to such programs is the protection of intellectual property and of other confidential or sensitive information. Combining our legal knowledge with well-tested project plans and consultative experience, we help our clients create and improve their records management programs cost-effectively.

BENEFITS AND RISKS

E-discovery readiness and electronic records management begin with a series of judgments about risk. Different industries, sets of exposures, business needs for information and organizational cultures are associated with different

judgments about how far organizations should go to preserve or destroy documents not required by law to be preserved. The decision to retain documents for a period of time on accessible company servers may be positioned, for example, as a trade-off with employees to discourage more unmanageable and perpetual end-user archiving on their work or personal computers, USB devices or other storage media. The risks of such personal storage include not only potential significant increases in the costs of discovery and risks of non-compliance with discovery requests, but loss of intellectual property, breaches of contractual confidentiality and breaches of personal information in violation of information security laws and triggering consumer notification requirements with their attendant significant business risks.

Increased compliance and litigation risks highlight the need for records management programs to be administrable. In some cases the old, extraordinarily detailed records management policies driven solely by regulatory requirements are being replaced by simpler ones based on judgments that the risk of retaining certain documents for periods of time beyond statutory timeframes is outweighed by additional administrative cost and risk of noncompliance due to the complexity of the program. The records management program that emerges reflects a balance between considerations of:

- ◆ Business needs and risk;
- ◆ Litigation risks; and
- ◆ Compliance risks (both regulatory requirements and the risk of non-compliance due to complexity).

Judgments must also be made about the extents to which the company will rely on technology as opposed to employees. Companies may choose to administer the record management program primarily through the training and management of end-users, but there is a clear trend toward greater reliance on technology and on administration of the records management program by a cadre of records managers, including culling of archives after messages are sent. Technologies available include tamper-proof archival systems and increasingly sophisticated tools for searching, filtering and tagging documents, for monitoring or auditing communications and for controlling non-compliant behaviors.

OUR APPROACH

A good project plan is critical to efficient records management and e-discovery readiness program planning and implementation. Our project plans are intended to prevent

redundant or repetitive activities both during and after the planning and implementation processes. Although those plans are always tailored to the needs of the client, and many steps may be unnecessary for your organization, a comprehensive project plan may be summarized at a high level as follows:

1. Organize a team including Legal, Compliance, Records Management, IT and (sooner or later) HR personnel, and establish agreement on critical issues and goals and project plan
2. Identify and evaluate records types unique to the organization (as opposed to, e.g., HR, tax and accounting records)
3. Search Track (may be conducted contemporaneously with Storage Track, #4)
 - ◆ Define options for (automatic or manual) search, tagging and/or filtering relating to different document types
 - ◆ Define options for e-discovery readiness
 - ◆ Litigation hold process
 - ◆ Metadata capture
 - ◆ Establishing chain of custody
 - ◆ Define options for monitoring and/or auditing compliance
 - ◆ Construct design and cost estimates
4. Storage Track (may be conducted contemporaneously with Search Track, #3)
 - ◆ Assess email storage requirements
 - ◆ Determine impact of imaging and other movement to electronic records on storage issues
 - ◆ Address concerns and opportunities relating to archiving by employees to their own computers or storage media
 - ◆ Define options for how documents will be stored
 - ◆ Define security and access needs
 - ◆ Construct design and cost estimates
5. Policy Development
6. Vendor Evaluation (including possible pilot test), Selection and Contracting
7. Solution Implementation
8. Development and Implementation of Training Programs for E-Discovery Readiness, Records Management and Document Creation, and of Monitoring Programs

WHY LORD, BISSELL & BROOK LLP?

Like all good records management counsel, we have extensive knowledge regarding legal retention periods, and a great deal of practical experience with the legal and business needs for records integrity and security. We also regularly

advise our clients on e-discovery issues and compliance with Sarbanes-Oxley, including avoidance of claims of spoliation of evidence. Our group is distinguished, however, by the skills of its members, including a former Big Four information management consulting practice leader, former IT professionals practicing IT law, e-discovery litigators and former general counsels. Drawing on these diverse and complementary skill sets, we strive to bring our clients the best that law and consulting firms can offer in the complex, interdisciplinary challenges of e-discovery and e-records: deep understanding of the subject matter and proven project management.

The Lord, Bissell & Brook Business Technology Group helps clients design, implement and execute tactics and strategies to navigate the rapidly changing eBusiness landscape, including all aspects of marketing, soliciting and completing business over the internet and via other electronic means.

The Business Technology Group includes lawyers with diverse backgrounds to effectively and efficiently respond to all client needs. We can help you exploit strategic opportunities and to protect your interests because we have the experience to help you execute your objectives. The Business Technology Group doesn't just help you compete, we help you win.

For additional information about our experience or to obtain additional information on how we may assist you, please refer to any of the Lord, Bissell & Brook Business Technology Group articles, or contact any of the lawyers at the end of this brochure.

ELECTRONIC RECORDS MANAGEMENT REPRESENTATIVE TRANSACTIONS

Our lawyers have advised clients on a wide variety of records, information management and e-discovery issues. Our services have included:

- ◆ Implementing eDiscovery readiness programs to reduce costs and risks and make best use of the changes to the Federal Rules of Civil Procedure effective as of December, 2006;
- ◆ Preparing comprehensive records management programs, including policies, procedures, guidelines and training modules for many financial services companies, technology companies, healthcare organizations, manufacturers and government agencies;
- ◆ Developing information management programs and records security policies for many financial services companies;
- ◆ Preparing electronic communications policies, computer

use policies and employee monitoring policies for numerous clients;

- ◆ Advising clients in connection with litigation-related records management issues, including spoliation;
- ◆ Preparing policies for issuing and enforcing legal holds post-Zubulake and creating legal hold notices for numerous clients;
- ◆ Advising many companies on the development and implementation of electronic records management solutions, including online systems for retaining and managing records subject to preservation orders;
- ◆ Advising clients on records management issues arising in connection with outsourcing and other third-party-related ventures;
- ◆ Negotiating and drafting contractual provisions, policies and procedures relating to privacy, security and information management;
- ◆ Preparing RFPs in connection with the outsourcing of information technology services and negotiating and drafting records storage agreements; and
- ◆ Advising companies on existing records inventories and making recommendations regarding retention or destruction of obsolete records.

Office Locations

ATLANTA

CHICAGO

LONDON

LOS ANGELES

NEW YORK

SACRAMENTO

WASHINGTON

www.lordbissell.com

THE BUSINESS TECHNOLOGY GROUP

Charlotte M. Bahin

Partner: Information management, banking, IT and eBusiness

Washington: 202.521.4106
cbahin@lordbissell.com

Michael E. Bieniek

Partner: Intellectual property, IT and eBusiness

Chicago: 312.443.0259
mbieniek@lordbissell.com

Brian T. Casey

Partner: Insurance regulation, privacy (GLBA and HIPAA) and eBusiness

Atlanta: 404.870.4638
bcasey@lordbissell.com

Sean C. Fifield

Partner: Intellectual property, IT and eBusiness

Chicago: 312.443.1787
sfifield@lordbissell.com

Matthew T. Furton

Partner: Business litigation, intellectual property, IT and eBusiness

Chicago: 312.443.0445
mfurton@lordbissell.com

Roy E. Hadley, Jr.

Of Counsel: Information privacy and security, intellectual property, IT and eBusiness

Atlanta: 404.870.4670
rhadley@lordbissell.com

Denise E. Hanna

Partner: Health care regulation and compliance, information management, technology, eBusiness

Los Angeles: 213.687.6709
dhanna@lordbissell.com

Patrick J. Hatfield

Partner: Insurance regulation, privacy (FCRA), intellectual property, IT and eBusiness

Atlanta: 404.870.4643
phatfield@lordbissell.com

Laura A. Kees

Associate: Intellectual property, IT and eBusiness

Atlanta: 404.870.4658
lkees@lordbissell.com

Paul T. Kim

Partner: Business litigation, intellectual property, IT and eBusiness

Atlanta: 404.870.4678
pkim@lordbissell.com

Kevin C. Lacey

Partner: Information management, privacy (HIPAA), information security, eBusiness and technology

New York: 212.947.4700
klacey@lordbissell.com

Kristine Lefebvre

Associate: Intellectual property

Los Angeles: 213.687.6735
klefebvre@lordbissell.com

Eric L. Marhoun

Of Counsel: Insurance regulation, variable product development and distribution, and eBusiness

Atlanta: 404.870.4624
emarhoun@lordbissell.com

Scott J. Moore

Partner: Information technology, software licensing, health and managed care, and outsourcing transactions

Los Angeles: 213.687.6702
smoore@lordbissell.com

Jon A. Neiditz

Of Counsel: Information management, privacy and information security, eBusiness and technology, compliance, insurance, human resources and health

Atlanta: 404.870.4684
jneiditz@lordbissell.com

Kevin M. Nelson

Associate: Electronic records management, intellectual property, IT disputes and litigation

Chicago: 312.443.1890
knelson@lordbissell.com

Jay G. Safer

Partner: Electronic records management, intellectual property, outsourcing transactions, information security and privacy, IT disputes and litigation

New York: 212.812.8305
jsafer@lordbissell.com

Amanda M. Witt

Associate: Intellectual property, information management, information security and eBusiness

Atlanta: 404.870.4685
awitt@lordbissell.com

This material may constitute advertising under certain codes.

© 2006 Lord, Bissell & Brook LLP