By Randolph A. Kahn and Lisa M. Douglas

MANAGING INFORMATION USING *reasonableness*

30-SECOND SUMMARY When it comes to dealing with information assets, what is reasonable in a world of heightened compliance expectations, reduced control over information resources, and often-competing interests? Courts have been evolving their approach to reasonableness in the context of information governance. Reasonableness for organizations with vast amounts of information now requires simplification of records retention rules, taking information management activities away from employees and allowing technology to play a greater role. Expecting employees to properly and consistently classify, store and retrieve information is inherently unreasonable given the volume of data most office workers confront on a daily basis. Organizations must rely on technology tools to ensure that records are not destroyed before policy allows, and evidence is available when required.

We live in a rapidly expanding information universe. While information is a major asset, when it becomes so voluminous that organizations are overwhelmed and can no longer harness its value (let alone manage it), something needs to be done. Many organizations are now facing the reality that their existing systems for managing information no longer work: They were developed in a tangible, paper-based world with much less volume and more physical user involvement. What was once a suitable approach is no longer viable and, indeed, has become increasingly impractical.

Our information-driven world is one of heightened compliance requirements along with reduced control over information, setting the stage for a different approach to information management. Organizations need to manage and contain their exploding universe of data while addressing legal and business risks, and they need to do so without spending exorbitant amounts of money. It seems appropriate to meet this challenge by adopting an evolved standard of reasonableness, a legal construct that has been applied in many different areas of law.

The expanding information universe and its costs

According to International Data Corporation (IDC), information storage growth is predicted to increase by 44 times in the next 10 years. More than 1.8 trillion gigabytes or 1,800 exabytes of new information was created in 2011 alone. To put this in perspective, an exabyte of data is equivalent to 50,000 years of DVD movies running continuously. The total amount of information created in 2011 nearly doubled what was created the year before.

The amount of new information is staggering, but says nothing about the current data mountain within most organizations. Information ceases to be an asset when there is so much of it that it can no longer be located, extracted, recalled, retrieved or utilized. Information becomes a liability when it is unorganized, inaccessible, uncontrolled and unprotected. Some executives assert that "storage is cheap" and the easy solution is simply to keep everything forever. However, while storage per gigabyte may be cheaper, overall costs are rising dramatically because there is so much more information. According to Gartner, "Worldwide data center hardware spending [was] forecast to total $106.4 billion in 2012, and surpass $126.2 billion in 2015."

Companies often consider only the simple, "direct" costs related to storage. They fail to consider ancillary amounts that show the true cost of information. In one example provided by AIIM, "It costs around 20 cents to *buy* 1GB of storage; however, it costs around $3,500 to *review* 1GB of storage." The remediation of privacy breaches constitutes another significant drain on resources. The *U.S. Cost of a Data Breach Study* (PGP Corporation and the Ponemon Institute, 2012) reports average total per-incident costs of over $6 million.

Volume is not the only complexity. There are more technologies, applications, formats, locations and clouds on which to float data.

To control the true cost and reduce risk exposure, companies must proactively manage information from the moment it is created or received until its final disposition. Yet the realities of information management force us to accept that the ways in which organizations have managed information in the past may no longer be prudent, practical or even possible. There is a compelling business need to develop the ability to effectively manage organizational information and control its unbridled growth. Businesses must improve their overall performance by curtailing costs required to support technology, management and litigation, while identifying and securing relevant business information when needed.

How are companies coping?

Many executives rank data growth as one of their top business challenges. Organizations are overwhelmed by having to do more with less. Employees are not able to manage information effectively. In many organizations, there is no information management policy framework to follow, and, where there is, it is not being audited or enforced. There is no technological panacea to solve these issues simply and elegantly.

It is not surprising that organizations are not coping well in our expanding and increasingly complex information universe, and that they are seeking solutions.

Information management by reasonableness

When it comes to dealing with information assets, these are challenging times for company stakeholders. IT professionals, lawyers, records managers and business executives are all confronted with an increasingly complex legal, compliance and technology landscape. We are forced to reconsider *what is reasonable* in a world of heightened compliance expectations, reduced control over information resources and (often) competing interests.

Consider that a large company may send and receive millions of email messages each day. While its policy may state clearly that "no email carrying personally identifiable information (PII) of customers shall leave the company without being encrypted," is it reasonable to expect that a manual review of all messages will be undertaken? Is it reasonable to expect employees to know what PII is, to know where it is and to make sure it is sufficiently secure? Would a court find it reasonable, if analytics software is used, to review email to address this issue? Would a court find it reasonable that, in the face of a policy to protect the PII, the

Randolph A. Kahn is a lawyer and founder of Kahn Consulting (*www.kahnconsultinginc.com*) and co-founder of Delve Information Technologies (*www.delve.us*). He is an educator, speaker, adviser and author of dozens of published works including "Information Nation." Kahn is a two-time recipient of the Britt Literary Award. *rkahn@kahnconsultinginc.com*

Lisa M. Douglas is a lawyer with the Toronto office of Baker & McKenzie LLP. A member of the firm's Information Technology and Communications practice group, she focuses on information governance including records and information management, privacy, data protection and security, ecommerce, cross-border data flows, lawful access and freedom of information. *lisa.douglas@bakermckenzie.com*

The authors gratefully acknowledge the research assistance of Eva Warden, an articling student with Baker & McKenzie LLP.

Should the determination of reasonableness change with the evolution or effectiveness of technology? Should it change because companies now produce so much information that managing this massive mountain of content is virtually impossible?

company's IT or information security department never provided encryption software to employees?

In response to a claim of sexual harassment, a governmental agency requests that the employer organization produce all complaints of sexual harassment, all communications in which employees sent or posted pictures of women or off-color jokes about women. Is it reasonable to expect employees to search for the relevant information? Would the answer be different if there were 50,000 employees and 50,000 laptop computers, 35,000 company smart phones, 50,000 email accounts, 50,000 voicemail accounts, 50,000 instant messaging accounts, 12,000 social network users authorized by the company, 9 petabytes of data and hundreds of IT systems around the enterprise? What if there were only 50 employees, one email system and very little information?

What will be deemed reasonable by a court or regulator is often fact-intensive. What facts mitigate in favor of a conclusion that a party's actions were reasonable? What if the actions taken by the party were the only practical solution — is that reasonable? What if the company policy, though it may seem reasonable, is in reality purely aspirational? What if the company's path is wholly untenable (due to high technology and labor costs) but, nonetheless, deemed to be reasonable by industry "best practices"? Should the determination of reasonableness change with the evolution or effectiveness of technology? Should it change because companies now produce so much information that managing this massive mountain of content is virtually impossible?

Aligning practices with technology

As a cost-saving initiative, the CIO of a US-based global enterprise enters into a multi-year deal with a third-party storage provider that will shift all electronic company information to the cloud.

The CEO has decided to outsource major HR functions to a company that will have control of employees' health information and other personal data.

The head of marketing and sales at an international financial services company has approved a new Social Networking Policy to allow marketing and offering for sale of a new life insurance product through Twitter and Facebook.

After years of "wasting" millions responding to discovery in lawsuits and producing vast amounts of information that should have been disposed of years ago, the general counsel has approved the acquisition of new technology that will automatically apply records retention rules to all types of e-records so that they are disposed of when their retention period is met without requiring employee attention.

The expanding information universe and reasonableness at law

Courts have long relied upon a reasonableness standard in the traditional records management context, generally requiring that, to be defensible, records retention policies must be reasonable considering all of the facts and circumstances surrounding the relevant documents, and must be instituted in good faith as a matter of policy and practice. Records management programs were the only legally defensible way a company could clean house and not fear claims for spoliation:

> " ... [W]e see no evidence of fraud or bad faith in a corporation destroying records it is no longer required by law to keep and which are destroyed in accord with its regular practices. As we have previously observed, storage of records for big or small businesses is a costly item and destruction of records no longer required is not in and of itself evidence of spoliation."
> — *Moore v. General Motors* (1996)

On the other hand, as demonstrated by the recent high-profile patent dispute between Apple and Samsung, failure to preserve all relevant evidence can be fatal in litigation. In this case, Samsung's failure to preserve needed email may have hurt its case in the eyes of the jury. Under the Federal Rules of Evidence, spoliation (intentional destruction of evidence) can lead to harsh consequences: an adverse inference (where the judge instructs the jury to infer that the evidence was destroyed because it was unfavorable to the party's case) or discovery sanctions (where a party can lose without a trial, i.e., default judgment). Following a successful motion by Apple, the jurors were instructed that they could presume that Samsung failed to preserve relevant evidence — specifically, all relevant email — favorable to Apple. The case resulted in a $1 billion verdict against Samsung.

Seven information management realities

1. Information is growing at an alarming rate.
2. Employees have no time for and are not very good at managing information.
3. Litigation response costs have increased sharply and show little sign of abating.
4. Over-retaining information increases legal risk and undermines business efficiency.
5. New technologies are introduced every year, yet few allow for simple, centralized management.
6. More company information is in the hands of third parties than ever before.
7. Organizations are awakening to the downside of keeping all information forever.

Organizations need to redouble efforts to build better legal hold processes. That said, and while the email should have been preserved in this case, is it reasonable to expect that truly "anything and everything" potentially relevant can really be preserved? Today, given the volumes and complexity of a large company's IT framework, something slipping through the cracks seems entirely likely. In that regard, while there is value in rethinking the litigation response process to strike an appropriate balance between being conservative and practical, a spate of new technologies has been developed to address various phases of the electronic discovery process to make an otherwise arduous and expensive process more manageable.

Courts do seem to be reacting to the challenges presented by our expanding information universe by evolving their approach to "reasonableness" in the context of information governance and applying it in new contexts beyond traditional records retention.

According to Judge Peck in the Feb. 22, 2012, opinion in *Moore v. Publicis Groupe*, "Computer-assisted review appears to be better than the available alternatives, and thus should be used in appropriate cases. While this Court recognizes that computer-assisted review is not perfect, the Federal Rules of Civil Procedure do not require perfection. … Counsel no longer have to worry about being the 'first' or 'guinea pig' for judicial acceptance of computer-assisted review." Other US cases have since continued this theme, asserting that while no review tool or process, manual or electronic, guarantees perfection, manually reviewing documents is prone to human error and inconsistencies. It is here that the tipping point is found, where the machine may be statistically more reliable than the human.

A recent freedom of information case points out that "custodians" cannot be relied upon to conduct exhaustive and effective electronic searches, suggesting that instead, as part of the emerging best practice, organizations "can (and frequently should) rely on latent semantic indexing, statistical probability models and machine learning tools to find responsive documents" (*National Day Laborer Organizing Network v. U.S. Immigration and Customs Enforcement Agency*, July 13, 2012).

Further leeway can be found in rules of civil procedure. Rule 37 of the Federal Rules of Civil Procedure provides a safe-harbor provision in the context of discovery, which provides that absent exceptional circumstances, a court may not impose sanctions on a party for failing to provide electronically stored information that has been lost as a result of the routine, good-faith operation of an electronic information system. This implies that imperfect electronic systems may be acceptable.

The courts in other countries are likewise taking note of the huge burden imposed on litigants required to produce relevant documents in the burgeoning information world of the 21st century. A review of recent jurisprudence reveals various examples. Rules in the United Kingdom require a "reasonable search" for documents to be disclosed. An Australian court reduced the scope of production required for practical reasons where the relevant electronic data repositories contained hundreds of thousands, if not millions, of documents, recognizing the high cost in time and resources associated with undertaking a broader review. A Hong Kong court cautioned against a standard of perfection in regards to the "properness" of records. In Canada, there has been growing judicial concern over the practical challenges, the risk of confidential or sensitive material being unnecessarily exposed, and the disturbing trend that the high cost of production is putting litigation beyond the economic ability of a vast number of litigants. Discovery in Canada is, therefore, tempered by the application of a proportionality standard or cost-benefit analysis, resulting in an implicit requirement that limits production to those records that are reasonably accessible.

Courts do seem to be reacting to the challenges presented by our expanding information universe by evolving their approach to "reasonableness" in the context of information governance and applying it in new contexts beyond traditional records retention.

After all, one of the themes emanating from the famous early articulation of "reasonableness" by Judge Learned Hand has been the concept of a cost-benefit analysis underlying the actions of the reasonable person, so as to avoid behavior that results in unacceptable costs.

Impact of "big data" on organizations

"The Information Explosion: How Organizations Are Dealing With It," a recent survey conducted by the Council for Information Auto-Classification (*www.infoautoclassification.org*), provides these insights:

- 71 percent of responding organizations have no idea what information they have in their stored data.
- 58 percent of organizations are keeping information indefinitely.
- 79 percent indicated that too much time and effort is spent manually searching for and disposing of information.
- 58 percent still rely on employees to decide how to apply corporate information-related policies (i.e., retention, privacy, security).
- Nearly half of organizations indicated that they are forced to re-create information because they cannot find it.
- 74 percent of organizations said valuable information is being lost (i.e., disposed, misplaced or unable to be found) due to the lack of proper technology solutions.
- 73 percent of respondents said their organization missed business opportunities because they cannot efficiently access information.

While there is precedent for relying on a "reasonableness" standard in developing global document management and review systems, it seems logical and defensible, from both a practical and a legal risk-management perspective, to apply this same standard to the management and disposition of the vast stores of information accumulated by business-as-usual processes. After all, one of the themes emanating from the famous early articulation of "reasonableness" by Judge Learned Hand has been the concept of a cost-benefit analysis underlying the actions of the reasonable person, so as to avoid behavior that results in unacceptable costs.

What is reasonable when it comes to records retention?

Historically, records management programs were built (if they were built at all) based on the content of information and the ability of employees to know their records and, therefore, manage them. That may have been fine when staff had a manageable number of paper documents to handle each day. But today, when the average office worker interacts with hundreds of information "nuggets" on a daily basis, and those nuggets are found in various forms and systems across a complex IT framework, that approach must change. For years, employees (sometimes records managers) were the gatekeepers for the identification of records to be retained, and would ensure that paper records were cataloged, boxed and carted-off to storage or destroyed at the end of their useful life.

Today, many organizations have deployed archiving and litigation technology solutions with the intent of providing records retention compliance and responsiveness to litigation. However, the basic premise of certain systems reinforces the "save everything" posture, which is untenable long-term for most organizations, and many of these solutions continue to depend on employee decision-making

ACC EXTRAS ON… Information management

ACC Docket
Leveraging Underused Data (Mar. 2013). *www.acc.com/docket/underused-data_mar13*

Quick Reference
Everyone's Nightmare: Privacy and Data Breach Risks (Jan. 2012). *www.acc.com/quickref/data-brch_jan12*

Leading Practices Profile
Leading Practices in Privacy and Data Protection: What Companies Are Doing (Aug. 2010). *www.acc.com/priv&dataprotect_aug10*

Presentation
Risk Management in the New Age of Scrutiny: Strategies, Tips and Guidance for In-house Counsel [Complete] (Nov. 2011). *www.acc.com/risk-mgmt-scrutiny_nov11*

Primer
DLA Piper Handbook on Data Protection Laws of the World (Mar. 2012). *www.acc.com/primer/data-laws_mar12*

ACC HAS MORE MATERIAL ON THIS SUBJECT ON OUR WEBSITE. VISIT *WWW.ACC.COM*, WHERE YOU CAN BROWSE OUR RESOURCES BY PRACTICE AREA OR SEARCH BY KEYWORD.

Seven steps to defensible disposition of information

A "REASONABLE" APPROACH TO USING TECHNOLOGY TO MANAGE BUSINESS CONTENT

1. Assemble a team of committed stakeholders representing key organizational interests, such as information management, legal, compliance, information technology and privacy, and ensure buy-in from senior management.
2. Identify the range of structured, semi-structured and unstructured data in the possession and control of the organization, and determine how it is generally collected, accessed, used and disclosed, and when it is deleted or destroyed (if at all).
3. Assess, test and acquire a commercial technology product/platform that is capable of running the analytics necessary to implement a disposition process covering all enterprise data subject to defined rules to be established by the assembled team.
4. Define and document the rules for retention and disposition of enterprise information based on a reasonable diligence process that meets the business needs and legal requirements for different types of information that have been identified.
5. Test, validate and refine the disposition system using actual data to confirm data integrity and that the results are reliable and capable of being audited; data retention and destruction must invariably be in accordance with the established rules.
6. Once the integrity of the system has been established, apply the disposition methodology to all enterprise information, understanding that some content can be disposed of with without classification while still maintaining a reasonable standard of diligence.
7. On an ongoing basis, verify and document the efficacy and results of the disposition program, and modify or augment the process as necessary.

By rethinking the retention rules to be applied, technology can be relied upon to do the job.

and action. Faced with this reality, advances in technology — combined with exploding data growth — are forcing a re-evaluation of core information management processes. In its simplest form, the choice falls to one of four categories:

1. Retain everything forever.
2. Dispose of everything tomorrow.
3. Let employees classify everything.
4. Let technology classify and people review.

When evaluating alternatives for managing information in the face of "big data," all of the available options should be considered. For example, if a company has an old shared drive and wants to migrate to SharePoint 2010, or wants to move to any email archiving tool from its current world of mismanagement chaos, what are the options for dealing with this mountain of information — some of it valuable, but much of it dated and no longer of any value? Certainly, it is "unreasonable" to move digital data junk from an old system to the new system, as this would be simply moving the problem of over-retention to a new environment — which only increases cost and reduces functionality. Organizations need to take advantage of systems migrations and application retirement to purge over-retained content in a legally defensible way — and the lawyers need to help.

One way that lawyers can help is to work more closely with other functional departments, such as information technology, records and information management, privacy and compliance, to ensure that their respective interests are better aligned, institutional knowledge is shared, and data is not only retained appropriately but also disposed of defensibly. Ultimately, the needs of all stakeholders can be met by purging data in a timely manner while adhering to simple yet properly articulated retention rules, and automating their implementation through effective analytic technology. To this end, many organizations are combining records/information management with privacy and security functions, while legal counsel is integrally involved as well. This integration of previously separate functions can reduce costs, improve compliance and generate the collective will to tackle "big data" head-on.

An important step in tackling "big data" is to move away from excessively detailed traditional records retention schedules and, instead, develop simple retention rules for much broader categories of business information including, where relevant, unified retention rules for regional or global enterprises. Exceptions to broadly applied rules can be made where necessary, but the

Examples of "big bucket" retention rules

ADMINISTRATION, BUDGETING AND ROUTINE MANAGEMENT
Records related to department administration, management, budgeting, support services and routine operations. Includes meetings and conference planning and support; general administration and management reports; general statistical, status and progress reports; general correspondence and reports that require no action; calendar and appointment books; trip requests; training program administration; task force and department meeting notes.

GENERAL ACCOUNTING: SUPPORTING RECORDS
Records and reports related to payment of financial obligations and to receipt of revenues and other income. Includes vouchers, invoices and statements; dividend payments; corporate charitable contribution payments; cost accounting; 1099s; expense reports; petty cash reports; check requests; proof of payment; account reconciliation; accounting for and allocation of revenue, costs, account reconciliation and routine reporting.

EMPLOYEE RECORDS: PERSONNEL RECORDS
Records related to individual employees that are maintained for the full term of employment. Includes employee's history of mandatory training; individual test results; employee certifications and licenses (such as registrations or licenses for accountants, auditors, engineers, attorneys, etc.); salary and wage changes; employment applications, employment offer letters and agreements; performance appraisals; resumes; confidentiality agreements; discipline records; termination documentation.

objective of simplicity is laudable from a cost perspective and reasonable from a compliance perspective.

Reasonableness for organizations with vast amounts of information requires simplification of records retention rules, taking information management activities away from employees to the extent practicable and allowing technology to play a greater role. For example, historically, retention rules were triggered by future events and tended to be rather granular, focusing on individual record types. By developing much higher-level rules and removing event triggers, technology is able to manage the lifecycle of information with little or no human intervention. In other words, by rethinking the retention rules to be applied, technology can be relied upon to do the job.

Organizations must rely on technology tools to ensure that records are not destroyed before policy allows, and that evidence is available when required. While technology is not perfect, it can perform substantially better than people can when strategically employed in the appropriate information management context. In any event, expecting employees to properly and consistently classify, store and retrieve information is inherently unreasonable given the volume of data most office workers confront on a daily basis.

Building a new information management paradigm

Organizations, with the help of their lawyers, records managers, IT staff and other stakeholders, should move away from a reactive "save everything" strategy that frustrates business efficiency and wastes valuable resources, with little or no corresponding business or legal benefit. Being able to say, "It wasn't destroyed" — even if (to be honest) there was no chance of finding it anyway — is not necessarily a benefit. Holding too much information is increasingly a detriment.

Implement a proactive information governance strategy, one that allows for the defensible disposition of information when retention requirements or preservation obligations have been satisfied. Otherwise, finding relevant documents or data in the ever-expanding information universe will be increasingly challenging, time-consuming, resource-intensive and truly impractical. Lawyers must rethink what is reasonable given the volume of information and complexities of managing it today. Doing nothing could be far worse in terms of organizational risk than moving forward with a strategy to manage and dispose of information that is reasonable, if not quite perfect in every way. Lawyers need to guide their corporate clients in the use of technologies to better manage information functions, such as records management, discovery and privacy processes, and refrain from aspirational policies with impractical solutions that cannot be implemented.

These are the days of truly big data. What was reasonable yesterday may not be tomorrow. Harnessing technology to be "faster, better and cheaper" and "legally compliant" is reasonable. Now is the time to seek practical, if not perfect, solutions, because the "perfect" solutions may not be attainable or reasonable. **ACC**