Applied Discovery® White Paper

Elements of a Good Document Retention Policy

By Courtney Ingraffia Barton, Esq.
Adapted for Canadian counsel by Wendy R. Cole, LL.B.

LexisNexis®

What Corporate Counsel Should Know About Retention and Destruction Policies for Digital Data: Elements of a Good Document Retention Policy

Document retention — especially the retention of electronic data — has become a hot topic in the legal profession. In the wake of several United States court decisions leading to high-dollar jury verdicts, and the increasing recognition of the importance of electronically sourced documents by the Canadian bench and bar, it is imperative that Canadian companies and their counsel start thinking about the retention and preservation of electronic information.

In the 21st-century business world, companies are creating and storing electronic documents and information at light speed. Consider the facts: over 99% of all documents created and stored are done so electronically, and approximately 60 billion emails are being created and sent each day according to the IDC[1]. Electronic information is not just found on desktops and laptops, either; it is captured by instant-messaging programs, housed on BlackBerry® devices, web sites, data recorders ... and the list of storage media continues to grow. Because electronic documents and information are easier to store, more information is being retained and archived on backup tapes and servers. But, for modern businesses, all of this electronic information can be expensive to store not only because of the cost of the physical storage of tapes, but because of the potential liability of keeping sometimes seemingly useless information too long — or not long enough. So how does a company balance the need to keep information for business purposes with what is required for the purposes of potential litigation?

What Is the Law?

In late 2005, the Discovery Task Force[2] released "Guidelines for the Discovery of Electronic Documents in Ontario."[3] In the Guidelines the DTF defined electronic discovery, or e-discovery, as "**the preservation, retrieval, exchange and production of documents from electronic sources in electronic form."**[4]

The Guidelines are premised on the fact that the existing *Ontario Rules of Civil Procedure*[5] already provide a legal foundation for the requirement that parties address issues relating to e-discovery."[6] Rule 1.03 of the *Ontario Rules* defines a document to include "data and information in electronic form." In January 2005, Rule 30.01(1) was amended to expand the definition of a document under that section as including "a sound recording, videotape, film photograph, chart, graph, map, plan, survey, book of account and data and information in electronic form."

Although Canadian jurisprudence on the topic of electronic discovery is still relatively sparse as compared to the American jurisprudence, "e-discovery is already widely used [in Canada] as an integral part of the discovery process in complex cases and, increasingly, in many types of litigation that are less complex."[7] Recent decisions in Ontario and British Columbia confirm that "a properly run company should have a documents retention policy requiring retention of files for a reasonable period extending beyond the limitation period for a civil cause of action in contract or tort and the limitation period for a reassessment under the *Income Tax Act*. Failure to do so risks a court making an adverse inference on the absence of evidence."[8]

[1] International Data Corporation (IDC) is an information technology research firm. [2] The Discovery Task Force ["DTF"] was a joint undertaking of the Ontario Superior Court of Justice and the Ontario Ministry of the Attorney General. [3] The Supplemental Discovery Task Force Report, dated October 2005, was prepared by the Task Force. The Supplemental Report includes Guidelines for the Discovery of Electronic Documents in Ontario, prepared by the e-discovery subcommittee ["Guidelines"]. [4] The Guidelines, pg. 1. [5] The *Ontario Rules of Civil Procedure, Courts of Justice Act*, R.R.O. 1990, Regulation 194 ("Ontario Rules"). [6] The Guidelines, pg. 1. [7] Ibid. [8] *Alvi v. YM Inc. (Sales)(cob Stitches)*, [2003] O.J. No. 3467 at para. 48 (Ont. Sup. Ct.) (QL); See also *336332 B.C. Ltd. v. Imperial Oil Ltd*., [2002] BCJ No. 844 at para. 47(B.C.S.C.) (QL).

Even before litigation is commenced, companies have a duty to preserve documents that may be relevant to pending or even potential litigation (often referred to as the litigation hold). As was stated in the DTF's Guidelines: "A party's duty to preserve electronically stored documents that are relevant to contemplated or threatened litigation arises in the same way as for paper documents."[9]

Some guidance as to the extent of a company's obligation to preserve and produce its electronic documents in the course of litigation is provided by the principles set out in the Guidelines. Principle number 5 states that "as soon as litigation is contemplated or threatened, parties should immediately take reasonable good faith steps to preserve relevant electronic documents. However, it is unreasonable to expect parties to take every conceivable step to preserve all documents that may be potentially relevant."[10] Principle 3 of the Guidelines provides that "in most cases, the primary source of electronic documents should be the parties' active data, and any other information that was stored in a manner that anticipates future business use, and that still permits efficient searching retrieval."[11] That being said, "if a party is aware (or reasonably should be aware) that specific, relevant data or information can only be obtained from a source other than the active and current archival data sources, then that source should at least be preserved and listed appropriately in the party's affidavit of documents for possible production."[12] Principle 4 goes on to state that "a responding party should not be required to search for, review or produce documents that are deleted or hidden, or residual data such as fragmented or overwritten files, absent agreement or a court order based on demonstrated need and relevance."[13] What is clear from the DTF's Guidelines is that the DTF recognized the need to balance the fact that significant relevant information is created and stored in electronic form and should be produced in litigation, with the fact that the volume of electronic information can be overwhelming and could potentially make litigation financially and logistically unmanageable (an access-to-justice issue). To strike that balance, the Guidelines suggest that, in most circumstances, companies will be obliged to produce only those electronic documents that are generally used and preserved in the course of the company's everyday business and that are reasonably accessible. Only if an opposing party can convince a court that a company's more obscure or inaccessible electronic information (such as deleted files, backup tapes or legacy data created on old or obsolete hardware or software) is relevant and necessary (if for example the opposing party provides evidence that suggests the party is willfully hiding or destroying relevant information) will the court demand that a company go to the effort and expense of restoring and producing items such as backup tapes, deleted files, and legacy data.

A Formal Policy Is a Must

First and foremost, companies should have a carefully crafted document retention policy that must be actively enforced and audited. A company's document retention policy must take into consideration not only business requirements, but the requirements of all applicable federal and provincial laws and regulatory rules respecting the retention of documents. Having a formal document retention policy that ensures a company keeps the appropriate electronic information for as long as is necessary — but no longer — is important for a number of reasons. First, adhering to a policy may limit liability in the long run. Many cases have been damaged due to the surfacing of unfavourable emails or documents kept too long and taken out of context. In many of those cases, had document retention policies been in place and enforced, that information would no longer be available.

[9] The Guidelines, pg. 5. [10] The Guidelines, pg. 11. [11] The Guidelines, pg. 10. [12] Ibid. [13] Ibid.

Second, if a document retention policy limits how long information is kept, companies will not only reduce the costs associated with storing documents, but will have less information to search and review when litigation arises. For example, if a company's policy is to hold on to documents for two years, then once a litigation hold is in place, there should only be two years of stored information that must be searched in order to find relevant documents. This can save a company time and money in the long run, as the most expensive part of any discovery phase is the time spent having lawyers review documents.

Policy as a Litigation-Preparedness Tool

A good document retention policy can also be used as a litigation-preparedness tool and will give in-house and outside counsel a roadmap to finding documents. In order to create a workable policy, companies must know where all of their documents and information are kept and how that information is stored. The American case of *Coleman (Parent) Holdings v. Morgan Stanley*[1] can be seen as a cautionary tale of a corporation (Morgan Stanley) that did not know where it stored and kept all of its electronic data. In May, after the company was found guilty of discovery abuses stemming primarily from its lack of knowledge about the location of its discoverable information, a jury awarded the plaintiff $1.4 billion in compensatory and punitive damages. While damages of that magnitude would not be awarded in Canada, the lesson is still important — a comprehensive document retention policy would have directed the company to its relevant documents.

Any policy should also state the name(s) of the custodian(s) of the information and should list the types of servers and backup tapes used. Creating a policy will require counsel to become familiar with the company's IT systems, which will be necessary if a court ever requires an explanation. Understanding the company's IT department can also prevent problems later on. Many corporate IT departments are not equipped to handle the volume of document retrieval that is often involved in litigation or government inquiries. Knowledge of the capabilities of the IT department will allow a corporation to hire outside vendors who can help archive data so that it is searchable later if needed.

Implementation and Flexibility

A document retention policy is only as good as its implementation. A policy needs to be rigorously enforced from top management down. Companies must make sure they educate their employees about not only the policy, but the implications of not following it. It must be easy to follow and periodically renewed, and it must clearly lay out how often it will be audited. The policy should also address the fact that employees may store and save information in different ways (i.e., some employees may save documents to a hard drive, others to a network) and on different hardware (some emails are only saved on BlackBerry devices and not in desktop or laptop inboxes). In addition, the policy must be flexible enough to be suspended if a litigation hold is necessary. The policy should address the litigation hold and how it is to be implemented, including any policy on email backup tapes. In summary, a document retention policy should:

- Be rigorously enforced from top management down
- Be created in conjunction with the IT and legal departments

[14] *Coleman (Parent) Holdings v. Morgan Stanley*. 2005 Extra LEXIS 94 (Fla. Ct. Mar. 23, 2005).

- Be easy to understandBe periodically updated
- Contain a formal auditing process
- Be easy to implement: employee education is key
- Address how employees store data
- Be flexible enough to suspend
- Address the possibility of a litigation hold
- Explain the company's IT systems
- Name the custodian(s)

Preventing Sanctions

In the end, when it comes down to litigation or a government information request, the most important reason for a company to have a workable and active document retention policy is so that it can persuade a court that documents that no longer exist were purged pursuant to a policy and not willfully destroyed and spoliated. Although it is uncertain whether spoliation will be recognized by Canadian courts as an independent tort[1], what is clear is that there are risks associated with the willful or even negligent destruction or alteration of evidence, including the risk that the court will draw an adverse inference or impose financial penalties if key evidence is destroyed.[2] If a company's policy is comprehensive and routinely audited, it can provide the court with assurance that a company has all of the information it is required to keep, and knows how to find it, which can go a long way to protecting a corporation in the long run.

We haven't heard the last word on this issue. As technology continues to change, so will the law.

About the Authors

Ms. Barton is Vice President, Industry Relations, at LexisNexis Applied Discovery. She is a former litigator with the United States Department of Justice and Arnold & Porter in Washington, D.C.

Ms. Cole is Product Manager, Applied Discovery, at LexisNexis Canada. She is a former commercial litigator with significant experience with large-scale documentary discovery. She can be contacted at **wendy.cole@lexisnexis.ca**.

[15] *Logon v. Harper*, [2003] O.J. No. 4098 at para. 42 (Ont. S.C.J.) (QL); *Rintoul Estate v. St. Joseph's Health Care Centre*, [1998] O.J. No. 4074 (Ont. S.C.J.) (QL); *Spasic Estate v. Imperial Tobacco Limited*, [2000] O.J. No. 2690 at para. 22 (Ont. C.A.) (QL) [16] Spoliation is a particular concern when dealing with electronic documents as electronic documents are susceptible to alteration. For example, even the simple act of making a copy of an electronic file can alter or damage the underlying meta-data in an electronic document (information respecting the date the document was created and edited, who it was created by etc.). To ensure that relevant meta-data is not altered or lost, the Guidelines suggest that "forensic copies" or "mirror images" that are specficially designed to preserve the integrity of the meta-data be made or that the relevant meta-data be captured from the original source documents before they are copied. The Guidelines, pg. 6.

For information about Applied Discovery, please contact
Wendy Cole at **wendy.cole@lexisnexis.ca** or **1-800-668-6481.**

The information contained herein is not intended to provide legal or other professional advice. Applied Discovery encourages you to conduct thorough research on the subject of electronic discovery.

LexisNexis®

LexisNexis Canada Inc.
123 Commerce Valley Drive East, Suite 700, Markham, Ontario L3T 7W8 CANADA