

Litigation Bulletin

April 2007

Managing Electronic Documents and Meeting Your Obligations When Litigation is Imminent

An overview for business leaders of the benefits of a document management policy to deal with the ever-growing volume of electronic documents.

Electronic Evidence and the Duty to Disclose During Litigation

The growing use of e-mail and the proliferation of computerized documents has resulted in businesses managing large quantities of records stored in a variety of different forms. These forms include magnetic tapes, diskettes, hard drives, hand-held devices like Blackberries and Palm Pilots as well as traditional paper documents, which may be printed multiple times.

When litigation is commenced or imminent, the “litigation hold” requires that parties preserve and disclose every document relating to any manner in issue.¹ The word “document” is defined broadly under the *Rules of Civil Procedure* of Ontario as including “data and information recorded or stored by means of any device”.² “Records” subject to preservation and discovery will include paper documents but also documents received, created or stored electronically within any electronic system, including individual computers, laptops, palm pilots, Blackberries, voice records, network file servers, zip drives, computer logs, back-up tapes and more.

The voluminous and volatile nature of electronic documents has made their preservation increasingly central to modern litigation. Failing to successfully implement a litigation hold may mean serious sanctions are imposed by the courts for spoliation.

The biggest problem with effectively implementing the litigation hold is the multitude of sources and the huge volume of electronic documents. The average hard drive on a per-

sonal computer is capable of storing the equivalent of a million pages of information or more. Today, the amount of electronic information stored at large corporations and the government is staggering. An Exxon Mobil lawyer estimated that Exxon Mobil stores 800 terabytes of information, which equates to 400 billion typewritten pages³.

Spoliation and Preservation of Electronic Evidence

Spoliation refers to the destruction, mutilation, alteration, or concealment of evidence,⁴ including the negligent destruction or loss of electronic evidence. Electronic evidence can be easily and permanently lost or changed, simply by booting up a computer, opening a file or installing new computer applications or data onto a hard disk, or copying data from one media to another. In addition, automatic document purging systems can lead to the destruction of otherwise relevant evidence such as e-mails. A litigant can suffer adverse consequences in terms of penalties that may be imposed by the Court for spoliation, costs and prejudice due to the loss or destruction of electronic evidence caused by the failure to preserve such evidence. Rule 30.08(1) of Ontario’s *Rules of Civil Procedure* provides that if a party fails to produce a document that is favourable to their own case, that party may not be able to use the document at trial, and if the document is unfavourable, the Court has the discretion to make any order it deems just.

Preservation of Electronic Evidence and Chain of Custody Issues

In circumstances where the authenticity and therefore the

admissibility of electronic evidence are likely to be in issue, additional steps should be taken to ensure that the preservation and collection of electronic evidence is sufficiently controlled to ensure its admissibility. An important part of authenticity is establishing the “chain of custody”, which is a process that verifies that information collected and copied was not altered in the copying process and has not been altered during any analysis. The term “chain of custody” refers to the controlled collection, movement, storage and access to and production of items of evidentiary value. Preserving and maintaining the integrity of electronic evidence is more difficult than paper-based records. If electronic evidence is copied from person to person without taking proper care how that information is copied, the risk of alteration is almost 100%. For example, in a situation where there is reason to believe that an employee’s laptop will contain evidence that supports a claim for theft of intellectual property, and IT staff sit at the computer and begin to review the documents, in doing so they have altered the last access date of those records.

Disputes concerning the admissibility and authenticity of electronic evidence tend to arise more frequently in circumstances where the “chain of custody” is important, such as cases involving fraud, theft of intellectual property or other criminal-like conduct, where for example, the individual is accused of stealing corporate secrets, confidential and/or proprietary information, downloading pornography at work or hijacking a Web-site. Other objections to the introduction of electronic evidence may stem from acknowledged or proven security lapses or breaches, where unauthorized access to the computer at issue or the computer network is known or becomes apparent. The controlled collection, movement, storage, access to and production of electronic documents helps to ensure that the “chain of custody” can be established.

Forensic evidence is most often required in these circumstances to establish or “authenticate” the electronic trail, to

prove that the impugned conduct took place and to establish the identity of the perpetrator, who often hides behind a pseudonym on the Internet.

There are a number of different programs and media that may be used. The method used must meet the following criteria:

- (i) It must meet industry standards for quality and reliability;
- (ii) It must be capable of independent analysis; and
- (iii) It must create tamper-proof copies.

All copies and originals should be labeled by time, date and source and stored in a secure place. All forensic analysis of the information collected should be done on a working copy created from the secure copy.⁵ Before copying information from the target computer, the computer must be virus checked with up-to-date virus checking utilities and before examining any media or making any copies, the originals must be “write protected”, so no data is added or changed during inspection and copying. Accurately copying all data on a drive requires making a sector-by-sector copy of the drive. This process creates a mirror image of the drive being copied, thus capturing all data, including residual data on the drive surface. Simply making a file-by-file back-up captures only active data and may be deemed inadequate for evidentiary purposes.

Putting in place the “Litigation Hold”

The lesson for Canadian business is to ensure that a comprehensive document retention policy is in place *before* it is needed; one that efficiently and effectively incorporates the concept of a “litigation hold” into the overall information management process. An important element of this is a protocol for saving and discarding documents received or created in the ordinary course of business. Such a protocol will

aid in litigation when documents were properly destroyed pursuant to the protocol in place. Conversely, failure to enact a protocol may undermine an organization's position in litigation when the destruction cannot be justified. Document retention policies usually consist of three separate phases:

- (a) destruction of unnecessary or duplicate records prior to filing, such as the destruction of extraneous copies of documents;
- (b) transfer of active files to long-term storage, such as when files are moved to off-site storage; and
- (c) Permanent destruction of files from long-term storage.⁶

Key Questions when Creating a Record Retention Policy

How long to keep a document, when and how to store the document, and how to dispose of the document, will depend on the type of document. Legal and regulatory requirements may also dictate what documents must be kept and for how long. The following inquiries should therefore be made in the course of developing a document retention policy:

- (a) Is there a legal requirement for keeping the document? Legal requirements include federal and provincial laws concerning various regulated matters, such as employment records, health and safety records, tax records, etc;
- (b) After the item is used for its intended purpose, what other purpose could it serve? Could it be used to support or oppose a position in an investigation or lawsuit? Could it support a tax deduction or balance sheet item? Could it support or explain a business decision?

- (c) What is the consequence of not being able to locate the document? If the document was destroyed pursuant to a records-retention program and no threat of litigation was pending at the time, the issue will be how reasonable the document retention/destruction program was. If the document is central to a lawsuit and is suddenly destroyed after litigation is commenced or threatened, the presumption will be that the destruction was accomplished deliberately.
- (d) Can the item be reliably reproduced elsewhere if needed? Is the information available from another database or source?
- (e) Once the possible use of a particular item is determined, the question becomes how long to retain the document. This question is answered by taking into account the relevant statutes of limitations, being the time period within which a lawsuit must be commenced for a particular claim after the basis for the claim is discovered, as well as any retention periods stipulated by law, such as income tax statutes.⁷

If adequate policies and procedures are in place to preserve relevant information, there may be no need to alter the organization's standard operating procedures when litigation is on the horizon.⁸

Outside of the litigation arena, an effective document retention policy can also reduce the burden/costs of storing irrelevant and obsolete documents, can assist in the identification and retrieval of documents, and facilitate the review of a large number of documents in an efficient manner. Another equally important purpose is to ensure that relevant and potentially useful records are retained; this serves to preserve corporate memory and enhance productivity.

Pallett Valo LLP Commercial Litigation Law Group

Our firm has the largest Litigation Department in Peel Region. We have the depth and expertise to provide legal advice and representation in complex litigation matters. Collectively, we apply a business approach to commercial disputes recognizing the benefits of litigation avoidance and early extraction strategies.

Our advice is designed to minimize and avoid risks through the use of negotiation and alternative dispute resolution mechanisms to resolve commercial disputes with a minimum of business interruption to our clients. However, there are times when our clients' interests are best served by knowledgeable and strategic advice coupled with decisive and aggressive action in the Courts. Our litigators have extensive trial and appellate experience and have fought numerous motions over injunctive remedies such as Mareva and Anton Piller Orders. We work closely with clients to develop and implement sound strategies geared toward achieving identifiable objectives while providing timely advice as to issues and options.

Contact Members of the Commercial Litigation Law Group at Pallett Valo LLP:

Anna Esposito aesposito@pallettvalo.com
Direct Dial: 905.273.3022 Ext. 260

Anne Kennedy akennedy@pallettvalo.com
Direct Dial: 905.273.3022 Ext. 204

Bobby Sachdeva sachdeva@pallettvalo.com
Direct Dial: 905.273.3022 Ext. 295

David Contant dcontant@pallettvalo.com
Direct Dial: 905.273.3022 Ext. 248

John Russo jrusso@pallettvalo.com
Direct Dial: 905.273.3022 Ext. 282

Maria Ruberto mruberto@pallettvalo.com
Direct Dial: 905.273.3022 Ext. 206

Michael Nowina mnowina@pallettvalo.com
Direct Dial: 905.273.3022 Ext. 285

Sophie Petrillo spetrillo@pallettvalo.com
Direct Dial: 905.273.3022 Ext. 214

Karen Groulx kgroulx@pallettvalo.com
Direct Dial: 905.273.3022 Ext. 281

The purpose of this document is to provide information as to recent developments in the law. It does not contain a full analysis of the law nor does it constitute an opinion of Pallett Valo LLP or any member of the Firm on the points of law discussed.

If you would like additional copies of the bulletin, or know of anyone who would be interested in joining our mailing list, please contact Marketing Coordinator at marketing@pallettvalo.com.

Rev.01/08

¹ *The Rules of Civil Procedure*, R.R.O. 1990, Reg. 194, Rule 30.02 (*Rules*); *Guidelines for the Discovery of Electronic Documents in Ontario* as submitted by Mr. Justice Colin L. Campbell to the Ontario Bar Association conference, "Electronic Discovery and The New ED Guidelines – A Roadmap for Dealing with Electronic Information, November 28, 2005 at pg. 1 (*Ontario Guidelines*)

² *Rules*, ibid. Rule 30.01. See also Rule 1.03 which states that 'document' includes data and information in electronic form", and 'electronic' includes created, recorded, transmitted or stored in digital form or in other intangible form by electronic, magnetic or optical means or by any other means that has capabilities for creation, recording, transmission or storage similar to those means, and 'electronically' has a corresponding meaning".

³ Ameet Sachdev, "E-mails become Trial for Courts: Costly Electronic Discovery – Part of Potentially Every Case in the 21st Century", Chicago Tribune, online edition, April 10, 2005

⁴ British Columbia Law Institute, "Report of Spoliation of Evidence" (2004) BCLI No. 34 at page 1.

⁵ Joan E. Feldman and Roger I. Kohn, "Electronic Discovery of Computer-Based Evidence" (http://www.forensics.com/html/trng_edu_articles.html).

⁶ Anson-Cartwright et al., "Records Retention: Law and Practice" (Toronto: Carswell, 2000) p. 1-2

⁷ "Document Retention Policies: Legal Reasons to Keep E-mail, Web-Pages and Other Records, by Barbara Weil Gall, reproduced on line at <http://www.gigalaw.com/articles/2000/-all/gall-2000-09-all.html>

⁸ *The Sedona Principles for Electronic Document Production*, January 2004, The Sedona Conference